GO-Global®

WINDOWS HOST

ADMINISTRATOR GUIDE

VERSION 4.0.1 • 3.30.2012

COPYRIGHT AND TRADEMARK NOTICE

Copyright © 1997-2012 GraphOn Corporation. All Rights Reserved.

This document, as well as the software described in it, is a proprietary product of GraphOn, protected by the copyright laws of the United States and international copyright treaties. Any reproduction of this publication in whole or in part is strictly prohibited without the written consent of GraphOn. Except as otherwise expressly provided, GraphOn grants no express or implied right under any GraphOn patents, copyrights, trademarks or other intellectual property rights. Information in this document is subject to change without notice.

GraphOn, the GraphOn logo, and GO-Global are trademarks or registered trademarks of GraphOn Corporation in the US and other countries. Microsoft, Windows, Windows NT, Internet Explorer, and Remote Desktop Services are trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. UNIX is a registered trademark of The Open Group. Sun Microsystems, Inc., Solaris, and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Portions copyright © 1998-2000 The OpenSSL Project. All rights reserved. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org). Portions copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved. This product includes software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Portions of this software are licensed from United Mindworks LLC.

MacBinary Toolkit for Java, Copyright 1998, 1999, 2001 by Gregory L. Guerin.
Available at http://www.amug.org/~glguerin/sw/#macbinary. All rights reserved.

All other brand and product names are trademarks of their respective companies or organizations.

Printed in the United States of America.

CONTACT INFORMATION

GraphOn Corporation
5400 Soquel Avenue
Suite A-2
Santa Cruz, CA 95062

Toll Free: 1.800.GRAPHON
Phone. 603.225.3525
Fax: 831.475.3017

GraphOn
Building A, Trinity Court
Wokingham Road
Bracknell, Berkshire
RG42 1PL
United Kingdom

Phone: +44 1344.206549
Fax: +44 1344.206855

CONTENTS

Chapter I — Introduction

Introducing GO-Global p. 1
GO-Global Features p. 1
New Features p. 3
System Requirements p. 3

Chapter II — Configuring the Host

Installing the GO-Global Host p. 5
Upgrading GO-Global p. 6
    Manually Copying the License File p. 6
Configuring the GO-Global Host for Web Clients p. 7
Modifying the GO-Global Web Pages p. 8
Installing the Web Files on a System other than the GO-Global Host p. 10
Redundant License Servers p. 10
    Three-Server Redundancy p. 10
    License-File List Redundancy p. 11
Configuring GO-Global to use a Central License Server p. 12
    Opening the License Manager Port in a Firewall p. 13
Configuring Support for Client Keyboards and/or IMEs p. 13
    Installing Additional Keyboards and IMEs p. 14
    Client Keyboard Mapping Files p. 16
    Keyboard/IME Identifiers Used by GO-Global p. 18
    Configuring Client Keyboard Options p. 18
    Specifying Layout Text Substitutions p. 18
    Setting the Fallback Layout Text p. 19
    Configuring Multiple Input Locales p. 19

Chapter III — Administering User Accounts

Administering User Accounts p. 22
Setting up User Profiles p. 22
Setting File Permissions p. 22
Setting up a Network Printer p. 23

Chapter IV — The Cluster Manager

The Cluster Manager p. 24
Managing Applications p. 25
Installing Applications p. 25
Adding Applications p. 25
Editing an Application's Properties p. 27
Duplicating an Application p. 27
Renaming an Application p. 27
Assigning Application Launch Parameters to Users or Groups p. 27
Removing Applications p. 28
Managing Sessions and Processes p. 29
Terminating a Session p. 29
Ending a Process p. 29
Shadowing a Session p. 29
Security Options p. 30
Selecting SSL Transport p. 30
Obtaining a Trusted Server Certificate p. 31
Using an Intermediary SSL Certificate with GO-Global p. 32
Creating Your Own Certificate Authority p. 32
Importing the Trusted Server Certificate on a Dependent Host p. 32
Creating a CA Key and Certificate p. 33
Creating and Signing Server Keys p. 35
Generating a CSR Using IIS Certificate Wizard p. 36
Notifying Users of a Secure Connection p. 36
Encrypting Sessions p. 37
Modifying the Host Port Setting p. 38
Standard Authentication p. 39
Integrated Windows Authentication p. 39
Password Caching on the Host p. 40
Password Caching on the Client p. 41
Password Change p. 42
Changing Passwords at Next Logon p. 42
Prompting Users to Change Passwords Before Expiration p. 43
Prompting Users to Change Passwords After Expiration p. 44
Password Change and Integrated Windows Authentication p. 44

Chapter IV — The Cluster Manager (continued)

Session Reconnect p. 44
Setting the Session Termination Option p. 45
Disconnecting a Session p. 45
Shared Account p. 46
Client Time Zone p. 47
Monitoring Server Activity p. 47
Viewing Session Information p. 47
Viewing Process Information p. 47
Refreshing the Cluster Manager p. 48
Setting the Refresh Rate p. 48
The Status Bar p. 48
Setting the Broadcast Interval p. 49
Session Startup Options p. 49
Applying Group Policy p. 49
Displaying Progress Messages p. 49
Logon Scripts p. 50
Setting Resource Limits p. 51
Specifying the Maximum Number of Sessions p. 51
Specifying the Minimum Physical and Virtual Memory p. 53
Session Shutdown Options p. 53
Specifying the Session Limit p. 53
Specifying the Idle Limit p. 53
Specifying the Warning Period p. 54
Specifying the Grace Period p. 55
Managing GO-Global Hosts from Client Machines p. 55
Keyboard Shortcuts for the Cluster Manager p. 56

Chapter V — Running GO-Global

Running GO-Global from a Computer's Desktop p. 57
Running GO-Global from a Web Browser p. 58
GO-Global Startup Parameters p. 59
Resizing the Client Window p. 61
Uninstalling GO-Global p.61
Automatic Client Updates p. 63
Updating the ActiveX Control and the Plug-in p. 64
Windows CE Client p. 65
Installing the Windows CE Client p. 65
Running the Windows CE Client from the Start Menu p. 65
Running the Windows CE Client from a Shortcut p. 66
Running the Windows CE Client from the Executable p. 66
Command-Line Arguments for the Windows CE Client p. 66
Uninstalling the Windows CE Client p. 67
Pocket PC Client p. 68
Installing the Pocket PC Client p. 68
Running the Pocket PC Client from the Start Menu p. 68
Running the Pocket PC Client from the GO-Global Executable p. 68
Using the Pocket PC Client p. 69
Uninstalling the Pocket PC Client p. 69

Chapter VI — Advanced Topics

Load Balancing p .70
Independent Hosts p. 71
Relay Servers p. 71
Dependent Hosts p. 72
Administering Relay Servers and Dependent Hosts on Different Networks p. 73
Host Selection p. 74
Relay Server Failure Recovery p. 74
Relay Server in a DMZ p. 74
GO-Global Host Performance Counters p. 75
Configuration Requirements for Delegation Support p. 76
Client Printing p. 79
Designating Access to Printer Drivers p. 79
Printer Configuration p. 81
Printers Applet p. 81
Adding and Removing Printers p. 82

Chapter VI — Advanced Topics (continued)

Setting the Default Printer p. 82
Editing Printer Settings p. 82
Printing a Test Page p. 83
Changing a Printer's Driver p. 83
Restoring Printer Settings p. 83
Mapping Printer Drivers p. 84
Client Printer Naming Customization p. 86
Client Clipboard p. 86
Client Sound p. 87
Client Serial and Parallel Ports p. 87
Client File Access p. 88
Remapping Client Drives p. 89
Hiding Client Drives p. 89
Hiding Host Drives p. 90
Mapped Drives p. 90
Multi-Monitor Support p. 90
Specifying the Maximum Color Depth for GO-Global Sessions p. 91
Disabling Image Compression p. 92
Obtaining the Name of the Client Computer p. 92
Application Script Support p. 93
Advanced Session Process Configuration p. 93
Proxy Tunneling p. 96
Proxy Tunneling via the HTTP CONNECT Method p. 97
Support for Internet Protocol version 6 p. 98
Enabling Support for PAE p. 98
Performance Auto-Tuning p.98
Automatic Windows Update and Hotfix Compatibility p. 99
Silent Installation p. 100
Log Files p. 100
Selecting a New Location for the Log Files p. 101
Setting the Output Level p. 101
Maintaining Log Files p. 102
Support Request Wizard p. 102

CHAPTER I

Introduction

1

Introducing GO-Global

GO-Global is the simple and secure application virtualization solution that extends the reach of existing Windows applications to corporate networks or the Web — without modifying a single line of code. GO-Global makes it easy to create a *private cloud* that allows authorized employees, business partners, and customers to securely access applications from anywhere, regardless of connection, location, client platform, or operating system. GO-Global is a complete application deployment solution that can be integrated and bundled with any 32-bit or 64-bit Windows application.

GO-Global Features

- **Network, remote dial-up, and remote Web accessibility.** GO-Global provides access to 32-bit and 64-bit Windows applications from GO-Global Hosts via the network, remote dial-up, or through Web access. This is managed through the Cluster Manager, and is transparent to the end user.

- **Cross-platform compatibility.** GO-Global provides access to any Windows application from virtually any client platform. Applications can be run from desktop computers such as Mac, Windows, and Linux—allowing users to work in their preferred computing environments. Windows-based applications deployed through GO-Global look, feel, and function as if they were running on a Windows operating system, regardless of the client platform.

- **Client file access.** GO-Global supports seamless integration of client drives, including hard disk and mapped network drives. This allows users to access files stored on the client computer and to save files locally.

- **Host monitoring.** GO-Global provides real-time monitoring of individual GO-Global Hosts, control of individual clients and processes, and logout and shutdown for individual users.

- **User roaming.** Internal and remote users can sign in to a GO-Global Host from any client workstation.

- **Automatic Windows Update and Hotfix Compatibility**. This feature automatically detects the locations of the internal operating system variables and functions used by GO-Global. This ensures that virtually every time the system is booted, users are able to start sessions and run published applications regardless of what Windows Updates and Hotfixes are installed on the system.

- **Session shadowing.** The session shadowing feature allows multiple users to view and control a single session and its applications. This feature allows help desk personnel and system administrators to help troubleshoot and debug user problems. Session shadowing may also be used for live collaboration.

- **Load balancing.** Load balancing distributes user sessions across multiple GO-Global Hosts. When load balancing is enabled, users can reconnect to a disconnected session running on any one of the load-balanced hosts.

- **Session reconnect.** With session reconnect enabled, GO-Global maintains client sessions on the server without a client connection. If a user deliberately disconnects from the server, or if the client's connection is lost due to network problems, the user's session and applications remain running on the server for the length of time specified by the administrator.

- **Performance Counters.** Performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. GO-Global Host performance counters allow administrators to monitor server activity from any machine with network access to a GO-Global Host.

- **Proxy Tunneling.** Proxy tunneling allows users to connect to GO-Global Hosts on the Internet via proxy servers.

- **Group Policy Support.** Using Microsoft's Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.

- **SSL Security.** GO-Global provides support for Secure Socket Layer (SSL) as a method for communication between GO-Global clients and servers.

- **Session Timeout.** Through the Cluster Manager administrators can specify time limits for the number of minutes that sessions are allowed to run on a GO-Global Host.

- **Inactivity Timeout.** Through the Cluster Manager administrators can specify time limits for the number of minutes of client inactivity.

- **Client Printer Name Customization.** Administrators can specify the format of client printer names and include information (including the user's name, the name of the session, and the client computer's IP address) in the name of the client printer.

- **Time Zone Redirection.** This option allows GO-Global sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the GO-Global Host.

- **Backward Compatible Client and Host**. This allows a client to connect to a GO-Global Host when the major and minor versions of the client and server match but the revision (service pack) or build numbers do not.

- **Automatic License Retrieval and Installation.** Using GO-Global's License Retrieval Wizard, administrators can automatically obtain a license file from the GraphOn license server and install the license file.

New Features

- **Support for 64-bit Windows.** GO-Global supports both 64-bit and 32-bit applications running on the x64 versions of Windows Vista, Windows Server 2008, and Windows 7.
- **Automatic Client Updates.** Administrators can configure GO-Global to automatically update Windows clients when users connect to a GO-Global Host that is running a newer version.
- **Simplified Client Printing.** Client printing has an updated, streamlined architecture with improved client compatibility, better integration with Windows hosts, faster session startup time, and support on 64-bit hosts.
- **Improved Application Compatibility**. GO-Global has a simpler interface to the operating system that provides enhanced compatibility with both x86 and x64 applications.
- **Faster Application Startup**. Per-process CPU and memory usage overhead are greatly reduced. As a result, applications start more quickly and consume less memory.
- **Dynamic Display Resize.** GO-Global automatically adjusts the size of the session's desktop when the user reconnects to the session from a different device or changes the resolution of the client device.
- **Client Sound.** GO-Global supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut.
- **Client Serial and Parallel Ports.** GO-Global allows applications running on the host to access client machines' serial and parallel ports.
- **Cloud Server Ready Architecture**. The GO-Global Host comes with built-in support for GO-Global Cloud. GO-Global Cloud provides a secure, high-availability gateway to GO-Global Hosts and includes enterprise-level authentication, access control, and load balancing features.

System Requirements

GO-Global Host

The GO-Global Host requires one of the following Windows operating systems:

- Windows Server 2008 Standard or Enterprise with Service Pack 2 (x86 and x64)
- Windows Server 2008 R2 Standard or Enterprise with Service Pack 1 (x64)
- Windows Server 2003 Standard or Enterprise Edition with Service Pack 2 (x86)
- Windows Server 2003 R2 Standard or Enterprise Edition with Service Pack 2 (x86)
- Windows XP Professional with Service Pack 3 (x86)
- Windows 7 Professional, Ultimate, or Enterprise Edition with Service Pack 1 (x64)
- Windows Vista with Service Pack 2 (x86 and x64)

Where applicable, these platforms are supported with or without the Security Rollup Package. Right-to-left languages are not supported.

GO-Global includes support for WoW64 ("Windows 32-bit On Windows 64-bit") which allows 32-bit applications to run on 64-bit versions of Windows.

GO-Global Administrators must have administrative rights on the host to perform the installation, and the host must have TCP/IP as a network protocol.

GO-Global listens on GraphOn's registered port 491 for TCP packets. Configure your external firewall and any software firewall on the host to allow TCP port 491.

GO-Global supports VMware ESXi and Hyper-V in Windows Server 2008 R2.

A Web Server (*e.g.,* Microsoft Internet Information Server (IIS) or Apache HTTP Server) must be available in order to set up the host for browser deployment of GO-Global.

The color depth of the client and host must be greater than 256 — 16 million or greater is recommended.

The Memory and CPU requirements of a GO-Global Host are determined by the applications that are published and the number of users accessing the system. In general, a GO-Global Host can support 12 "heavy" users/500 MHz CPU and 25 "light" users/500 MHz CPU. ("Heavy" is defined as a user running one or more large applications with continuous user interaction. "Light" is defined as a user running one application with intermittent user interaction.)

GO-Global supports a maximum round-trip latency of 500 milliseconds.

GO-Global Client

Users can connect to a GO-Global Host from any computer that supports a GO-Global client. GO-Global supports the following platforms:

- Windows XP, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Vista and Windows 7. With the exception of Windows 2000, which is 32-bit only, both the x86 and x64 versions of these operating systems are supported.
- Red Hat Linux (Enterprise Linux 4 and 5) and SUSE Linux (Enterprise Desktop 10.) Only a 32-bit client is provided. When installing this client on a 64-bit operating system, additional 32-bit dependencies may need to be installed. Consult your distribution's documentation for details on how to do this. Installing the client via a meta-packager such as yum will automatically fetch and install these dependencies for you.
- Mac OS 10.4 and later.
- Pocket PC 2003 and Windows Mobile 5.
- Windows CE 4.2 or later on Mitsubishi's TX120 device and Mintwave's ACC-Lite and ACC-mini devices. SEH (the C++ Structured Exception Handling component) and RTTI (the Run-Time Type Information component) are required to run GO-Global on a Windows CE device. To determine if these components exist on the device, open ceconfig.h found in the Windows folder.

  On a Windows CE 4 device, if the following lines:
  #define COREDLL_CRT_RTTI 1
  #define COREDLL_CRT_CPP_SEH 1
  are included in this file, RTTI and SEH are supported.

  On a Windows CE 5 device, if the following line:
  #define COREDLL_CRT_CPP_EH_AND_RTTI 1
  is included in this file, RTTI and SEH are supported.

GO-Global supports the following browsers:

- Apple Safari 5.0.6 or later on Mac OS X
- Mozilla Firefox 3.6 and 10.0.3 (ESR) on Windows
- Mozilla Firefox 3.6 on Linux (x86 only)
- Internet Explorer 6.0 or later on Windows

CHAPTER II

Configuring the Host

2

Installing the GO-Global Host

GO-Global is delivered as a self-extracting executable and can be installed by double-clicking the executable. It can also be unpacked and installed by running **gg-host.windows_x86.exe** or **gg-host.windows_x64.exe** in the root folder where it was unpacked. The setup installs all of the GO-Global Host files as well as the files necessary to configure the GO-Global Host for browser logons.

The setup includes a **License Retrieval Wizard** which will automatically retrieve and install a license for GO-Global if there is no existing license. If you already have a valid GO-Global license, the License Retrieval Wizard will not launch.

You will need the Product Code supplied by your GraphOn sales representative in order to complete the License Setup. If you do not have a Product Code and wish to obtain a temporary demo license, type **demo** in the **Product Code** box.

You can obtain a license at any time after installation by clicking Start | Programs | GraphOn GO-Global 4 | License Retrieval Wizard.

Notes: Minimum permissions for the license file(s) (in C:\Program Files\GraphOn\GO-Global\Programs*.lic) are:
Administrators: Full Control; **Users**: Read & Execute; **SYSTEM**: Full Control

If the following error message appears in a Log file, it is possible that the permissions are incorrect for the license file:

```
FlexLM code #-1; FlexLM text: Cannot find license file. The license files
(or license server system network addresses) attempted are listed below.
Use LM_LICENSE_FILE to use a different license file, or contact your
software provider for a license file.)
```

When combining two GO-Global licenses or when using two separate licenses on the same GO-Global Host, the hostnames in the license files are case-sensitive and must be identical.

After installing GO-Global and running the License Retrieval Wizard, you will need to restart the host and then verify that the **Application Publishing Service** and the **License Manager** are running.

To verify that the Application Publishing Service and License Manager are running

1. Click the **Start** button on the Windows taskbar.
2. Click Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Find **GO-Global Application Publishing Service** and **GO-Global License Manager** in the list of services.
5. Verify that these services have "Started" and that the Startup is "Automatic."

If you would like to set startup preferences for the GO-Global Host, choose GO-Global Application Publishing Service from the list, and click the **Startup** button. Select the options you want to apply to the GO-Global Host.

Upgrading GO-Global

When upgrading from GO-Global for Windows 3.2, running the GO-Global 4 Host installer automatically uninstalls version 3.2 and backs up existing GO-Global settings, including the list of published applications and host options. These settings are fully restored during the 4.0 installation. A new license is required to run the 4.0 host. Customers who are not current must contact their local reseller or sales@graphon.com.

Cluster Managers on host running GO-Global for Windows version 3.2 are unable to display or administer hosts running GO-Global 4, and vice versa. GO-Global Hosts running different versions of GO-Global do not recognize each other.

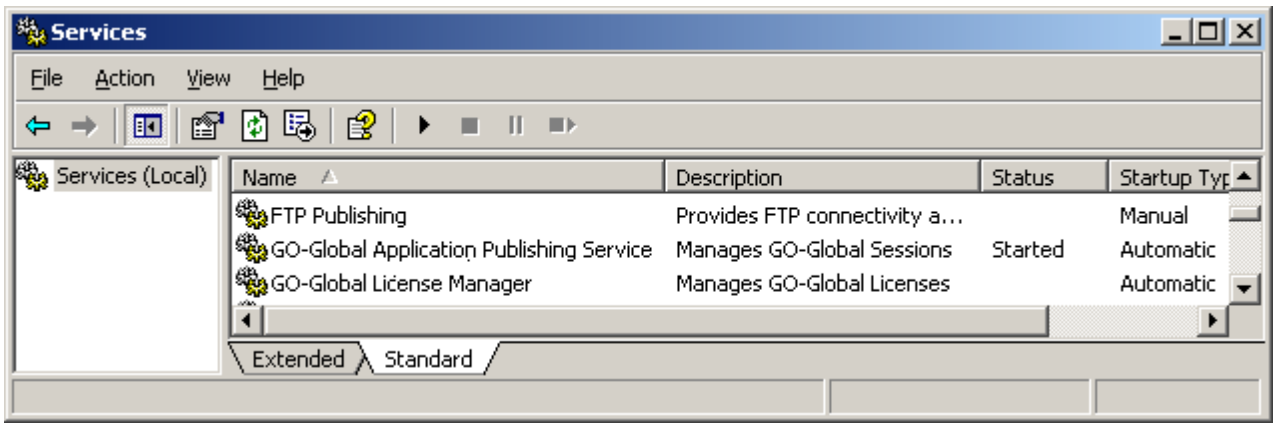
Manually Copying the License File

If you choose not to run the **License Retrieval Wizard**, you can copy your license file into the Programs directory in the GO-Global install path. If you have configured GO-Global to use a central license server, copy the license file to the license server. (For more information, see the section ***Configuring a Central License Server*** below.)

Once the license file has been copied over, you will need to stop and restart the **License Manager**.

To start the License Manager

1. Click the **Start** button on the Windows taskbar.
2. Click Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Select **GO-Global License Manager** from the list of services.
5. Click the **Start** button.



Note: Restarting the License Manager will not affect existing sessions running on the GO-Global Host.

Configuring the GO-Global Host for Web Clients

The GO-Global Host setup installs the GO-Global Web files under C:\Program Files\GraphOn\GO-Global\Web. If Microsoft Internet Information Services (IIS) is detected during installation, a virtual directory will be created in IIS that points to the GO-Global Web files. If IIS is not available, administrators will need to manually host the GO-Global Web folder contents on the specified Web server.

For more information on virtual directories in IIS, see http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/8c110149-8060-4dd7-9bdb-e262c21483dd.mspx?mfr=true

Administrators can edit the GO-Global HTML pages to modify default options and limit which clients are made available to users. During installation, the initial Web page is set to logon.html. Users accessing the host from a Web browser should be directed to the GO-Global logon page. (For example, http://hostname/goglobal/logon.html)

Logon.html automatically detects the user's platform and browser and runs the appropriate GO-Global Client. The clients.html page also detects the user's platform and browser, but it lists all the GO-Global clients that can be installed on the user's computer. The allclients.html page lists all GO-Global clients no matter which client operating system is detected.

In addition to logon.html, clients.html, and allclients.html, the following HTML pages are located in the GO-Global Web folder:

HTML Page	Description
index.htm	Default landing page.
installCE.html	Install page for the Windows CE Client.
installLinux.html	Install page for the Linux Client. (gg-client.linux.rpm)
installMac.html	Install page for the Mac OS X Client. (gg-client.mac.dmg)
installWindows.html	Install page for the Windows Client. (gg-client.windows.exe)
installPPC.html	Install page for the Pocket PC Client.
web.config	Used to indicate that logon.html is a default document for the virtual directory, and to indicate that file browsing is disabled for the virtual directory. (The web.config file only exists when Microsoft IIS 7 or later is installed.)

Note: In earlier versions of GO-Global, separate HTML pages were provided for the different browser plug-ins and for different combinations of GO-Global options. For example, embeddedactivexlogon.html was used to start GO-Global in Internet Explorer with the embedded window option, and looselinuxpluginlogon.html was used to start GO-Global in Firefox on Linux with the loose window option. In GO-Global 4, a single Web page, logon.html, supports all of the browser and configuration options. Therefore, there is no need for these additional, configuration-specific Web pages, and they are no longer included in the product.

Modifying the GO-Global Web Pages

You can use the above HTML pages as-is to install and run GO-Global from its supported operating systems and browsers. You can also customize these pages or create new pages to meet your specific needs. Modifications can be simple cosmetic changes that modify the appearance, text or images of the pages. Or changes can be as complex as pages that are dynamically generated by Web applications. The following examples illustrate a few of the ways you can customize GO-Global's Web pages.

- **Example 1**: Remove platform and configuration options from existing pages

To remove links to the client for Windows CE

1. Edit allclients.html or clients.html in a text editor.
2. Delete the following lines from the file:

```
else
{
            document.write('<a href="installCE.html">Windows CE
Client</a><br>');
}
```

3. Save the file.

To prevent the embedded windows option from being presented to users running Internet Explorer

1. Edit allclients.html or clients.html.
2. Modify the following lines from:

```
if(browser.msie)
{
       document.write('Microsoft ActiveX Control: <a
       href="logon.html?direct=true">Loose</a> | <a
       href="logon.html?direct=true&embed=true">Embedded</a><br>');
}
```

to:

```
if(browser.msie)
{
       document.write('Microsoft ActiveX Control: <a
       href="logon.html?direct=true">Loose</a><br>');
}
```

3. Save the file.

- **Example 2:** Create a Web page with links to specific applications

To create a page with links to Wordpad and Windows Explorer:

1. Open a new or existing Web page in an HTML editor.
2. Click the editor's **Insert Hyperlink** option.
3. Type in a hyperlink to a Wordpad document:

   http://hostname/goglobal/logon.html?mode=embed&app=C:\Program%20Files\Windows%20NT\Accessories\wordpad.exe&args=C:\Users\Public\Public%20Documents\welcome.rtf

4. Type in the display text for the hyperlink, e.g., "Welcome."
5. Repeat Steps 2-4 to create a link to Windows Explorer:

http://hostname/goglobal/logon.html?mode=embed&app=C:\Windows\System32\explorer.exe

6. Save the file and add it to your Web server path.

In this example, GO-Global options are specified in hyperlinks to the logon.html page. When users click on these links, logon.html reads these options from the hyperlink and loads the appropriate client with the specified options.

- **Example 3:** Create a page that loads a specific application

Logon.html lets users create their own hyperlinks and specify whatever GO-Global options they like. In some cases, you may not want users to have this capability. For example, you may want to prevent users from opening any application or file on the host computer and instead provide a page that loads a specific application with a fixed set of options.

When specifying the application, you can use the Display Name that appears in the Cluster Manager or the fully qualified path to the application.

To only allow users to run a specific application with specific options

1. Open logon.html in a text editor.
2. Replace all instances of GetVarDecoded("variable") with either an empty string (“”) or the desired value for the parameter.
3. For the “app” variable, enter the application’s Display name that appears in the Cluster Manager. For example:

   ```
   var app = "Wordpad";
   var args = "";
   ```

   or enter the fully qualified path to the application. For example:

   ```
   var app = "C:\\Program Files\\Windows NT\\Accessories\\wordpad.exe";
   var args = "";
   ```
4. Save the file.
5. If desired, rename the file. (E.g., wordpad.html)

When using a fully qualified path, any application-specific arguments must be specified using the `var args` parameter, regardless of whether or not the application was published via the Cluster Manager.

Notes:

The Plug-in will not run if Microsoft Internet Information Server (IIS) 6.0 is installed on a GO-Global Host running Windows Server 2003 or Windows Server 2008, unless you modify IIS to serve a document with an extension that does not have a registered MIME type on that server. See Microsoft Knowledge Base article 326965 for more information: http://support.microsoft.com/default.aspx?scid=kb;en-us;326965

For GO-Global purposes, type .xpi in the **Extension** box on Windows systems and .dmg on Mac systems. In the **MIME Type** box, type **application/octet-stream**. Restart the World Wide Web Publishing Service on the Web server after making this change.

More information about GO-Global hyperlink parameters and how to specify them is provided in Chapter 5.

Installing the Web Files on a System other than the GO-Global Host

You can install the GO-Global Web files on a system other than the GO-Global Host.

To install the Web files on a system other than the GO-Global Host

1. Copy the contents of the \Program Files\GraphOn\GO-Global\Web directory to the desired Web server.
2. Edit the logon.html page on the Web server and add the following statements, inserting the address of the GO-Global Host in place of hostname.

```
if (host.length == 0)
{
        host="hostname";
}
```

Redundant License Servers

If you wish to use redundant servers, select stable systems as server machines. Do not pick systems that are frequently rebooted or shut down. Redundant license server machines can be any supported GO-Global Host machines. These servers must have excellent communications on a reliable network and need to be located in the same subnet. Avoid configuring redundant servers with slow communications or dial-up links.

GO-Global supports two methods of redundancy:

- Via a set of three redundant license servers
- Via a license-file list in the LM_LICENSE_FILE environment variable

Note: The License Manager service should be disabled on secondary servers of Central License Servers and Three-Server Redundant License Servers.

Three-Server Redundancy

With three-server redundancy, if any two of the three license servers are up and running, a "quorum" of servers is established, and the system is functional and serves its total complement of licenses.

Three-server redundancy is designed to provide hardware failover protection only and does not provide load-balancing. This is because with three-server redundancy, only one of the three servers is **"master"** and capable of issuing licenses.

Following is an example of a three-server redundant license file that GraphOn supplies after registering online. You must provide the hostnames of the three GO-Global Hosts as well as the hostids (Ethernet addresses, in most cases) for each. The port of the license server (e.g., 27000) must also be appended to each server line, if it is not already listed.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
DAEMON blm
INCREMENT session blm 4.0 31-dec-2012 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 4.0 31-dec-2012 uncounted D1D222D031C4 \
HOSTID=ANY
```

The three-server license file needs to be copied to each of the three license servers.

Lastly, you must point the GO-Global Host to the license server. This can be done in two different ways, either by copying the license to each GO-Global Host and editing it to use USE_SERVER (see example below), or by adding each server to the environment variable.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
USE_SERVER
```

With the second option, add each server to the environment variable, using commas to separate the servers. For example, LM_LICENSE_FILE = 27000@wilson,27000@piper,27000@caspian. Restart the **GO-Global Application Publishing Service** and the **GO-Global License Manager** on the "master" server first (wilson, in the example above), then on the secondary and tertiary servers.

We recommend running Flexera's **lmtools** application to check the status of the redundant license servers once all three servers are up and running. Launch lmtools.exe and select the **Server Status** tab. Click on **Perform Status Enquiry** and verify that your servers are "UP."

You can obtain lmtools from the Programs directory (\GO-Global\Programs) or from: http://www.globes.com/support/fnp_utilities_download.htm#downloads. The lmtools application is included for diagnostic purposes. Any questions on its functionality should be directed to Flexera.

License-File List Redundancy

As an alternative to three-server redundancy, license-file list redundancy is available when there is limited system administration available to monitor license servers, when load-balancing is required for applications located far apart (e.g., Chicago and Tokyo), or when two or more license servers are required.

With license-file redundancy, each one of a group of license servers serves a subset of the total licenses. As such, this method does not provide true redundancy in the way three-server redundancy does.

Set the **LM_LICENSE_FILE** environment variable to a list of license files, where each license file points to one of the license servers. GO-Global attempts a license checkout from each server in the list, in order, until it succeeds or gets to the end of the list.

The following example illustrates how license-file list redundancy works. If ten licenses are desired, you will need to request two sets of product codes with a count of five for each set from a GraphOn sales representative. The actual licenses will be generated from the product codes. Unlike with three-server redundancy, the server machines can be physically distant. The license servers on both servers need to be running.

The sample license files will look like:

License 1 for chicago:

```
SERVER chicago 00508BFE7FFE 27000
DAEMON blm
INCREMENT session blm 4.0 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
       user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
       Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
       1996-2012 GraphOn Corporation. All Rights Reserved" ck=142 \
       SN=12865-AA
INCREMENT any_app blm 4.0 permanent 5 1DF84A360E8F HOSTID=ANY \
       user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
       Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
       1996-2012 GraphOn Corporation. All Rights Reserved" ck=84 \
       SN=12865-AA
```

License 2 for tokyo:

```
SERVER tokyo 00508BF77F7E 27000
DAEMON blm
INCREMENT session blm 4.0 permanent 5 16BE40E1D98D HOSTID=ANY \
      user_info="Joe User joeu@mycompany.com" ISSUER="GraphOn \
      Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
      1996-2012 GraphOn Corporation. All Rights Reserved" ck=142 \
      SN=12865-AA
INCREMENT any_app blm 4.0 permanent 5 6DB6F3E402DF HOSTID=ANY \
      user_info=" Joe User joeu@mycompany.com " ISSUER="GraphOn \
      Corporation" ISSUED=17-feb-2012 NOTICE="Copyright (C) \
      1996-2012 GraphOn Corporation. All Rights Reserved" ck=84 \
      SN=12865-AA
```

The administrator of the chicago server should set **LM_LICENSE_FILE** to: 27000@chicago;27000@tokyo where 27000 represents the port that the license servers in Chicago and Tokyo are running. This will direct the license engine to first attempt license checkouts from **chicago**. If unsuccessful, it will attempt to checkout from **tokyo**.

The administrator of the tokyo server should set **LM_LICENSE_FILE** to: 27000@tokyo;27000@chicago. This will direct the license engine to first attempt license checkouts from **tokyo**. If unsuccessful, it will attempt to checkout from **chicago**.

To change or set the LM_LICENSE_FILE variable

1. To view or change the current Environment Variables, right-click **My Computer** and select **Properties**.
2. Select the **Advanced** tab and click **Environment Variables** below.
3. Under **System variables**, select LM_LICENSE_FILE and click **Edit**.
4. Change the **Variable value** from **C:\Program Files\GraphOn\GO-Global\Programs** to reflect the new redundant servers. Separate the license server names with a semicolon (;). GO-Global will attempt the first server in the list. If that fails for any reason, the second server is tried.
5. Restart the **GO-Global Application Publishing Service**.

As with three-server redundancy, we recommend running **lmtools** to verify the status of the redundant license servers once all servers are up and running.

Configuring GO-Global to use a Central License Server

Two methods can be used for configuring GO-Global to use a license server that serves multiple machines. In the following examples, machine550 is the name of the license server and machine-w2k is the name of the GO-Global Host. We recommend stopping the GO-Global License Manager on the GO-Global Host before getting started. The License Manager should be disabled on all secondary servers of the Central License Server.

To stop the GO-Global License Manager

1. Click the **Start** button on the Windows taskbar.
2. Click Control Panel | Administrative Tools.
3. Double-click **Services**.
4. Select **GO-Global License Manager** from the list of services.
5. Click the **Stop** button.

Once you have stopped the GO-Global License Manager on the GO-Global Host, you may proceed with one of the following methods for configuring a central license server:

On the GO-Global Host, place port@host (e.g., 27000@machine550) in the LM_LICENSE_FILE environment variable instead of the path to the license file. FLEXnet Publisher's LMTOOLS.EXE reports that the license file on machine550 is being read correctly.

—or—

On the GO-Global Host, place USE_SERVER directly after the SERVER line in the license file on the GO-Global Host. This is essentially the same as the preceding method but the change to the environment variable is not required.

For example, the permanent license file (e.g., license.lic) on GO-Global Host (MACHINE-W2K) would appear as follows:

```
SERVER machine550 00d0b74f4023
USE_SERVER
```

Opening the License Manager Port in a Firewall

If there is a firewall between the GO-Global Hosts and the license server, the ports for FLEXnet (27000, by default) and for the license manager (BLM) need to be open in the firewall. For the license manager, add

```
port=<port#>
```

to the license on the license server for a specific port. (Unless you manually assign a specific port number, an ephemeral port number is used.)

EXAMPLE:

```
SERVER caspian 000476BA8F74 27000
DAEMON BLM port=5678
INCREMENT session blm 4.0 31-dec-2012 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 4.0 31-dec-2012 uncounted D1D222D031C4
HOSTID=ANY
```

Configuring Support for Client Keyboards and/or IMEs

Windows uses input languages, keyboard layouts, Input Method Editors (IME), and code pages to map keys on a keyboard to the characters on the display. When a key is pressed on the client's keyboard, GO-Global sends a key code to the host, which translates the key code into a Windows input message using the session's active keyboard layout. The GO-Global setup configures the host to support clients that use the same operating system, keyboard, and/or IME as the host. GO-Global supports clients with different operating systems and keyboards with keyboard mapping files.

The following section describes mechanisms and procedures to manage keyboards and IMEs in sessions on client computers that do not match the host system.

Installing Additional Keyboards and IMEs

Before clients can use keyboards and/or IMEs that are different from the host's, the files used to support them must be installed on the GO-Global Host. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not.

To install keyboard layouts on a host running Windows XP or Windows Server 2003

1. From the Start menu, click Control Panel.
2. Double-click the **Regional and Languages Options** icon.
3. Click the **Languages** tab.
4. In the **Supplemental language support** box, click the check boxes next to the desired language groups.
5. Click **OK**.

Additional files will be copied to your machine. You may need to provide the OS install CD or the network share name.

Support for the new languages will become available after restarting.

Note: Windows XP with Service Pack 2 supports a number of input locales that are not available on Windows Server 2003, Windows Vista, or Windows 7. Make sure the GO-Global Host's operating system can support all the input locales required by all users.

To install keyboard layouts on a server running Windows Server 2008

1. From the Start menu, click Control Panel.
2. Double-click the **Regional and Language Options** icon.
3. Click the **Keyboard and Languages** tab. Then click the **Change keyboards...**button.
4. In the **Text Services and Input Languages** window, click the **Add...** button to add the desired language(s). Select the language(s) by clicking the check boxes in the **Add Input Language** window.
5. Click **OK**.
6. Click the **Apply** button in the **Text Services and Input Languages** window.
7. Click **OK**.

The following is a list of keyboards that each GO-Global client supports.

The **Linux Client** supports:

Linux Keyboard Layout Name(s)	Linux Keyboard Layout	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	us	English (United States)	US	00000409	us.kbm
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	jp.kbm
French	fr	French (France)	French	0000040C	fr.kbm
Belgian (be-latin1)	be	French (Belgian)	Belgian French	0000080C	be.kbm
German, German (Latin1), German (Latin1 w/ no dead keys)	de	German (Germany)	German	00000407	de.kbm
Polish	pl	Polish	Polish (214)	00010415	pl.kbm
Brazilian (ABNT2)	br	Portuguese (Brazil)	Portuguese (Brazilian ABNT2)	00010416	br.kbm
*See the **Client Keyboard Mapping Files** section below for more information.					

The **Mac OS X Client** supports:

Mac OS X Keyboard Layout Name	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S.	English (United States)	U.S. International	00020409	us.kbm
French	French (France)	U.S. International	00020409	fr.kbm
German	German (Germany)	U.S. International	00020409	de.kbm
*See the **Client Keyboard Mapping Files** section below for more information.				

Note: Due to physical differences between the Mac OS X and Windows keyboards, the Mac OS X keyboard mapping files use the **U.S. International** Windows keyboard layout to translate a majority of the keys to Windows applications.

The **Windows CE Client** supports:

Windows CE Keyboard Layout Name	Windows CE VM Language	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
English US	en	English (United States)	US	00000409	*internal*
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	ja_JP.kbm
French	fr	French (France)	French	0000040C	fr.kbm
German	de	German (Germany)	German	00000407	de.CH.kbm
*See the **Client Keyboard Mapping Files** section below for more information.					

Windows clients (including the native Windows Client, the ActiveX Control, and the Plug-in) support any keyboard that the GO-Global Host has drivers for.

Client Keyboard Mapping Files

The GO-Global Client uses keyboard mapping files on Linux, Mac OS X and Windows CE to ensure that the proper keyboard layout is loaded on the host and that the correct key codes are sent for each key press and release. Keyboard mapping files allow support for new keyboards to be added by simply copying a new keyboard mapping file to the client. Keyboard mapping files are installed into the **/etc/gg-client/kbd** directory of these clients. An internal version of the **us.kbm** keyboard mapping file will be used if a keyboard mapping file is not found.

These clients can automatically load keyboard mapping files based on information obtained from the operating system.

The Keyboard Mapping File Installation Locations (i.e., default root paths)

Client OS	Native Install	Browser Plug-in Install	Default Layout	Layout Obtained by…
Linux	/etc/ gg-client/kbd	~/.mozilla/ gg-client/kbd	U.S. English	Environment variable or automatically from the OS
Mac OS X	/etc/ gg-client/kbd	/etc/ gg-client/kbd	U.S.	Environment variable or automatically from the OS
Windows CE	/GraphOn/GO-Global Client/kbd	N/A	en	Automatically from the OS

Environment Variable	Description
GG-CLIENT_KBD_FILE	This environment variable is used to specify the fully qualified path name of the mapping file to use. If specified, this will override all other means of obtaining the filename path. For example: On Linux, **GG-CLIENT _KBD_FILE= /home/someuser/KeyMappingFiles/MyCustomKeyMappingFile.kmf** will cause that exact file to be loaded. If that file is not found the internal version of the **us.kbm** keyboard mapping file will be used.
GG-CLIENT_KBD_FILE_ROOT	This environment variable is used to specify the root path name to the keyboard mapping files. The **kbd** directory that contains the keyboard mapping files will be expected to be in this directory. For example: On Linux, **GG-CLIENT _KBD_FILE_ROOT=/home/someuser**, will cause the file /home/someuser/kbd/*xxx*.kbm to be loaded, where '*xxx*' indicates the LAYOUT obtained from the following GG-CLIENT _KBD_FILE_LAYOUT environment variable or automatically from the OS.
GG-CLIENT_KBD_LAYOUT	This environment variable is used to specify which LAYOUT (or file name prefix) to use. This LAYOUT name along with the appended .kbm extension will be used as the file name. For example: GG-CLIENT_KBD_LAYOUT= MyCustomKeyMappingFile will load the file /ect/gg-client/kbd/MyCustomKeyMappingFile.kbm. If the above example for GG-CLIENT_KBD_FILE_ROOT is also used, the file /home/someuser/kbd/ MyCustomKeyMappingFile.kbm will be loaded. A subdirectory of the root path name to the mapping files can also be included here. For example: GG-CLIENT_KBD_LAYOUT=thinclient/us will load /etc/gg-client/kbd/thinclient/us.kbm provided a different root path is not specified. This will override the LAYOUT obtained automatically from the OS.

Notes:

Previous versions of the Linux Client use the command-line argument -kb and the plug-in/applet parameter "keyboard" to inform the server of the correct keyboard layout. For example, **-kb 0000040C** would override the environment variable **LANG = en_US** and cause the server to use the **French keyboard layout**. This is no longer recommended. Each keyboard mapping file contains the correct **keyboard layout** value that the server should use. Specifying a different **keyboard layout** with the command-line argument **-kb** or the plug-in/applet parameter **"keyboard"** could cause the keys to operate in undefined ways.

The command-line argument -kb and the plug-in/applet parameter "keyboard" can still be used to load an IME by specifying a **layout text**. For example, **-kb "Japanese Input System (MS-IME2002)"** can be used to load the Japanese IME available with Microsoft Office XP and Windows XP.

Keyboard/IME Identifiers Used by GO-Global

GO-Global uses two identifiers, collectively known as **GO-Global Input Identifiers** (GGII), to specify a keyboard/IME for a session. The first is a keyboard layout. These are 8-digit string identifiers that Windows operating systems use to load keyboard drivers and IME programs. They are similar to locale IDs in that the last four digits typically match the 4-digit locale ID of the language supported by the keyboard. Keyboard layouts that specify an IME typically start with an "E". The list of available keyboard layouts can be viewed in the registry under the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts] key.

The second identifier used by GO-Global is the layout text string, which is a registry value of each keyboard layout registry key. These strings are displayed in the dropdown box under Keyboard layout/IME when adding input languages.

In the following examples, the first has a keyboard layout GGII of 00000409 and a layout text GGII of US. The second example has a keyboard layout GGII of E0010411 and a layout text GGII of Japanese Input System (MS-IME2002).

EXAMPLES:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\00000409
  Layout File = KBDUS.DLL
  Layout Text = US

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\E0010411
  Ime File = imejp81.ime
  Layout File = Kbdjpn.dll
  Layout Text = Japanese Input System (MS-IME2002)

Configuring Client Keyboard Options

You can specify the keyboard/IME for a session using the -kb shortcut parameter or the "keyboard" hyperlink parameter. These take both types of GGIIs described above. On Windows computers, if the -kb shortcut parameter is not specified, GO-Global will use the layout text of the currently active keyboard layout. On Linux computers, GO-Global does not send a layout text to the server if one is not specified on the command-line.

EXAMPLE:

Windows shortcut using a keyboard layout:
gg-client.exe -h server1 -kb 00000409

Specifying Layout Text Substitutions

Layout text substitutions can be specified on the server to map between client and server keyboard layout names. They can be used to:

1. Overcome differences in layout text names on different versions of Windows. For example, the **Japanese Input System (MS-IME2000)** layout text from a Windows 2000 GO-Global client system can be substituted with the **Japanese Input System (MS-IME2002)** layout text from a GO-Global Host running Windows Server 2003.
2. Substitute an ANSI name for a keyboard layout that has a UNICODE name. For example, when specifying a keyboard layout with a UNICODE name through the "keyboard" applet parameter in an ASCII HTML page, it is necessary to substitute an ASCII name for the UNICODE name.

Keyboard Layout Substitutions are specified under the [HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Keyboard\Layout \Substitutes] registry key. Each REG_SZ value within this key has the name of a GGII, and the value is the name of a layout text from the server that should be used in place of the client name.

Setting the Fallback Layout Text

If there is no GGII specified from the client, or the one specified fails to load a valid keyboard layout, the GO-Global Host uses a fallback mechanism to determine which keyboard layout should be used for the session. The fallback layout text should be the layout text for the keyboard layout that will be used by all clients connecting to the server, exclusive of those passing a valid GGII. The fallback layout text is automatically set during installation if the keyboard layout that is active is an IME. It may be modified after installation by editing the **Fallback Layout Text** value under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\System\Keyboard Layout

Note: When connecting to a Chinese GO-Global Host, the **Sign In** dialog appears from the shortcut along with the IME bar specifying Chinese as the default language. Clicking CTRL+spacebar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users will be unable to type a user name and password.

Configuring Multiple Input Locales

The **Default User** account profile can be configured with different and/or multiple input locales. Account profiles for new users logging on to a GO-Global Host are automatically configured with the **Default User** account's input locales. Users can switch to any input locale that is defined in their account profile.

Note: Users with roaming profiles or profiles that already exist on the GO-Global Host will not receive these new settings. These accounts must be configured manually.

As an example, the following instructions describe how to install and use the German input locale on an English Windows Server 2003.

1. Enable German on an English Windows Server 2003.

1.1 Sign in to the GO-Global Host interactively with a user account that you wish to set the Input Local for.

1.2 Click Start | Control Panel | Regional Language Options.

1.3 Click the **Languages** tab.

1.4 Click **Details**.

1.5 On the **Text Services and Input Languages** dialog, click **Add**.

1.6 On the **Add Input Language** dialog, expand the list of **Input languages** and select **German (Germany)**.

1.7 In the **Keyboard layout/IME** box, note that this has been changed to German. This indicates that the physical keyboard should be German. If the physical keyboard is not German, select the appropriate keyboard layout and click **OK**.

1.8 On the **Text Services and Input Languages** dialog, click **OK**.

1.9 On the **Regional and Language Options** dialog, click the **Advanced** tab. Click the **Apply all settings to the current user account and to the default user profile** check box.

1.10 After reading the **Change Default User Settings** message, click **OK**.

1.11 On the **Regional and Language Options** dialog, click **OK.**

2. Verify that the input locale is correctly installed and configured.

2.1 Launch **Notepad** in this interactive session.

2.2 Type a few characters in English.

2.3 Type Left Alt + Shift.

2.4 Type a few characters and verify that they display in German.

The German input locale is now enabled for the **Default User** profile and the user that was logged on to the system in step 1.1.

3. Switch between input locales during a GO-Global session.

3.1 Start a GO-Global client and connect to the server with the account used in step 1.1.

3.2 Launch **Notepad**.

3.3 Type a few characters in English.

3.4 Type Left ALT + Shift.

3.5 Type a few characters and verify that they display in German.

Notes:

Users will not be able to switch input locales when the **Sign In** dialog is displayed. The input locale for the default language of the GO-Global Host will be used.

On Windows clients, the selected input locale of server-based applications is *not* displayed in the system tray of the client computer.

CHAPTER III

Administering User Accounts 3

Administering User Accounts

To access applications on a GO-Global Host, clients must sign in to the host machine. When users start a GO-Global client, they are prompted for their user name, password, and the name of the host they wish to access. This information is optionally encrypted and passed to the Application Publishing Service running on the GO-Global Host. The Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user signs in to a host and a domain is not specified, the GO-Global Host first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the **User name** box of the **Sign In** dialog. For example, NORTH\johng.

When a local user name on the GO-Global Host is the same user name as a domain account, each with a different password, GO-Global treats them as two separate accounts. Consider, for example, the following scenario:

- A local account on the GO-Global Host **johng** with a password of **local**
- A domain account **johng** with a password of **domain**

When typing user name, **johng** with the password **local** in the **Sign In** dialog, the account will authenticate on the local GO-Global Host. When typing **johng** with the password **domain** in the **Sign In** dialog, GO-Global does not attempt to authenticate on the domain, but fails with an invalid user name or password. You must specify the domain name in the User name field in the **Sign In** dialog. For example, NORTH\johng.

Once a user is signed in, GO-Global relies on the host's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights that have been granted to individual user's sessions.

Users must be able to log on interactively (locally) on the GO-Global Host. Assign local logon rights to users in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

This chapter contains basic information regarding the administration of user accounts on the GO-Global Host. For more detailed information, please consult Windows Help, accessible from the Start menu.

Setting Up User Profiles

Most Windows applications store user specific settings and files under the user's Windows profile. By default, Windows creates a local profile for each user that logs on to a system. A local profile is specific to a given computer and will not work well if you are running multiple GO-Global Hosts. If you are running a multi-host environment, you should set up roaming user profiles. A roaming profile is stored centrally and can be accessed from any networked computer for which that profile is valid. When a user with a roaming profile logs on to any networked computer, the desktop will appear exactly as the user left it the last time he or she logged off. For multi-host environments, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

Notes:

A profile is only valid on the platform for which it was created. For example, a Windows XP profile can only be used on a Windows XP computer.

For a step-by-step article describing how to create roaming user profiles in Windows Server 2003, see Article ID 324749 in Microsoft's Knowledge Base (http://support.microsoft.com/kb/324749). For Windows XP, see Article ID 314478 (http://support.microsoft.com/kb/314478).

Setting File Permissions

As the system administrator, you may need to restrict user access to certain files and resources. Keep in mind that there are multiple users accessing the host. Particularly in a load-balanced server environment, we recommend write-protecting system and application folders so that users are unable to save files on a local GO-Global Host. Otherwise, the next time a user logs on to GO-Global and is routed to a different server, the files and folders will be inaccessible.

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders. File permissions can only be set on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

Tip: While in Windows Explorer, choose the **Help** button or press **F1** for more information on setting file permissions.

Setting up a Network Printer

As the administrator, you can set up network printers for use by GO-Global clients. You must first create a port on the GO-Global Host that connects directly to the host and then install the printer locally. This provides direct access to the printer.

To add a port to the GO-Global Host

1. Click Start | Settings | Printers.
2. Double-click **Add Printer**.
3. Select local printer, then click **Next**.
4. Click **Create a new port** and select **Standard TCP/IP Port** as the type. Click **Next**.
5. Type the printer's IP address, as prompted by the printer wizard.
6. Select the printer manufacturer on the left and the printer model on the right, or click **Have Disk**.
7. Follow the directions provided by the wizard to install the proper printer driver.

CHAPTER IV

The Cluster Manager

4

The Cluster Manager

The Cluster Manager allows you to administer, monitor, and control client access to the GO-Global Host. The Cluster Manager displays a list of the users signed in to a GO-Global Host, along with the applications the users are running, and the time the application was started. Through the Cluster Manager, you can perform a variety of administrative tasks, such as adding and removing applications, terminating user sessions, and ending processes running on the host.

To access the Cluster Manager

Double-click the Cluster Manager icon on the desktop.
–or–

1. Click the **Start** button on the Windows taskbar.
2. Click Programs | GraphOn GO-Global 4 | Cluster Manager

The left panel of the Cluster Manager lists the hosts on the network running the Application Publishing Service. By default, the Cluster Manager displays information for the host running on your machine. To connect to other hosts and view information about them, click the host name from the list of GO-Global Hosts.

If a host's icon has a red x, the administrator does not have administrative rights on the host. If the host's icon has a red x and is grayed out, the host is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that host from the Cluster Manager.

Click the **All Hosts** icon in the left panel of the Cluster Manager to view a list of all active sessions on the network. This allows you to view active GO-Global sessions without connecting to individual hosts. This is also helpful for locating a particular session's host.

You must belong to the Administrators group on each GO-Global Host in order to access that host from the Cluster Manager. Without administrative rights on a host, you will be unable to add applications and terminate processes, etc.

Managing Applications

For clients to run an application via GO-Global, the application must be added to the Cluster Manager. Clients are then able to connect to the GO-Global Host and access the application.

Installing Applications

When installing applications to be run through GO-Global, please consult the vendor's documentation for instructions on proper multi-user installation. You will likely need to install the application under an administrative account, but installation requirements will vary depending on the application. Installation should also adhere to Microsoft's guidelines for multi-user deployment. It is recommended that applications be installed on drives formatted with the Windows NT file system (NTFS). If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

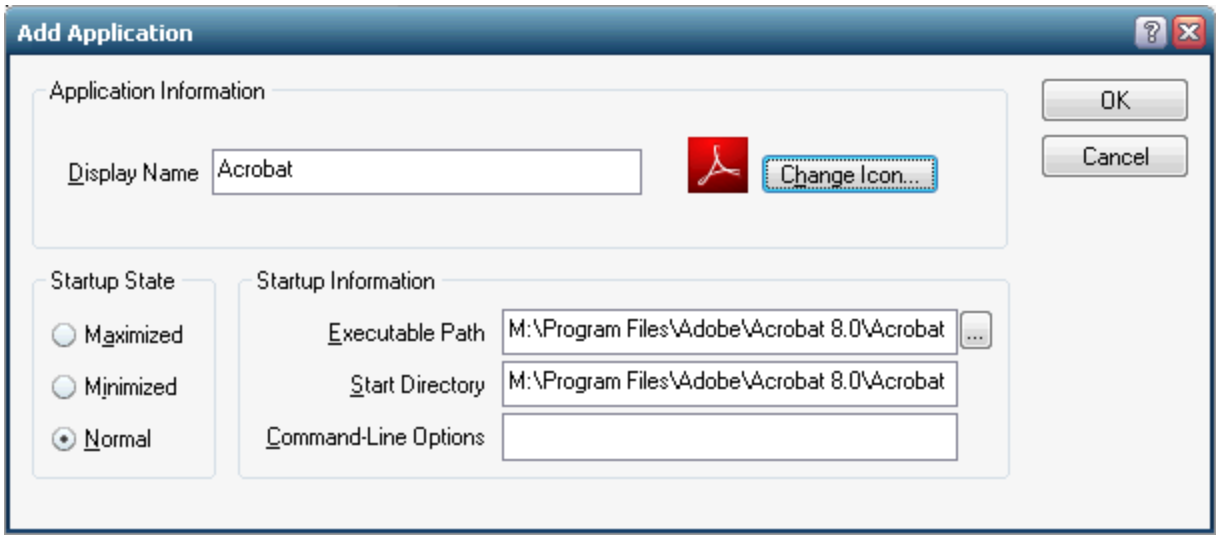
Note: Please note that deploying applications via GO-Global does not entitle your enterprise to unlimited access rights. You must still abide by the vendor's licensing agreement with regard to the number of applications that can be run concurrently.

Adding Applications

Applications must be added to the Cluster Manager before users can access them. When adding applications to the Cluster Manager, you can specify startup parameters that control how the application opens and what processes are initiated when the application is started.

To add an application to the Cluster Manager

1. Select the desired host from the list of **All Hosts**.
2. Click the **Applications** tab.
3. Click the **Add** button.
4. Click the **Browse** button next to the **Executable Path** box to locate the application's executable file.
5. If you browsed for the application's .exe file in the preceding step, the file name will automatically be entered in the **Display Name** box. (This application name is displayed to users in the Program Window.) You can keep the default display name or you can type a new one. The application's Display Name cannot consist entirely of spaces and it cannot contain a backslash (\). This field cannot be left blank.
6. If you browsed for the application's executable file, the pathname of the directory will automatically be displayed in the **Start Directory** box. Otherwise, type the full pathname of the directory in which you want the application to start.
7. In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
8. In the **Command-Line Options** box, you can specify launch parameters for the application. Because these parameters are specific to each application, please refer to the application's documentation for information about specific launch parameters.
9. Click the **Change Icon** button if you would like to select an icon other than the application's default icon.
10. Click **OK** when you are finished.



After registering an application with the Cluster Manager, the application's name and path will appear in the list of **Installed Applications**. You can sort items in the list in ascending or descending order by clicking the column's title. This holds true for all lists in the Cluster Manager.

If you want to set up applications that use ODBC data sources, you must set up the ODBC drivers as system DSNs (data source names), in order for GO-Global clients to be able to access the data sources. For more information about data sources, consult the Windows ODBC Data Source Administrator online Help.

Due to access restrictions, the Cluster Manager cannot verify the validity of paths specified in UNC format (e.g., \\Machine Name\Folder Name\...) or that reside on a mapped network drive. If the Executable Path or Start Directory of a published item involves a mapped drive or is specified with a UNC path, the Cluster Manager will accept the specified path regardless of whether or not it is valid. If the path is invalid, or if the client user does not have rights to access the specified executable file or folder, the published item will not appear in the Program Window. Select the item and click the **Properties** button. Try updating the item's Executable Path or its Start Directory. If the item has been uninstalled or moved to a new location, it will not be displayed in the Cluster Manager when the Application Publishing Service has been restarted.

The Cluster Manager is unable to display group and user settings for any item's path specified in UNC format or that resides on a mapped drive. The following message is displayed in the Cluster Manager's Application Users/Groups window for any application or file where this applies: "User/Group settings not available."

If an item that resides on a mapped drive but is not licensed for use with GO-Global is published in the Cluster Manager, the item's icon will appear in the Program Window. However, the user will be unable to open the item and will receive an error message when attempting to launch it.

Tip: Click the right mouse button on an item in the list of Installed Applications or the list of Application Users/Groups to display shortcut menus of the most frequently used commands.

Editing an Application's Properties

Once an application has been added to the Cluster Manager, you can edit the application's properties at any time. For example, you can edit the application's startup state, the location of its executable file, or the folder from which you want the application to start.

To edit an application's properties

1. Click the **Applications** tab.
2. Select an application from the list of **Installed Applications**.
3. Click the **Properties** button.
4. Do any of the following:
   - In the **Executable Path** box, type a new pathname.
   - In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
   - In the **Command-Line Options** box, type any startup parameters for the application.
   - In the **Display Name** box, type a new display name for the application.
   - In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
   - Click the **Change Icon** button to browse for a new application icon.

Duplicating an Application

Duplicating an application makes an exact copy of the selected registered application. This is useful if you want to make the same application available to different users or groups but with variations. For instance, you may want to register one version of an application with command-line options to bypass the **Sign In** dialog, and another version without command-line options that requires clients to sign in. When duplicating an application, you are required to select a new display name.

To duplicate an application

1. From the list of **Installed Applications**, select the application you would like to duplicate.
2. Click Tools | Applications | Duplicate.
   –or–
   Click the **Duplicate** button to the right of the list of Installed Applications.

Renaming an Application

The display name that you assign to an application will appear to the end user in the Program Window. You can change an application's display name at any time.

To rename an application's display name

1. From the list of Installed Applications, select the application you would like to rename.
2. Click Tools | Applications | Rename.
   –or–
   Click the **Rename** button to the right of the list of Installed Applications.

Assigning Application Launch Parameters to Users or Groups

The Cluster Manager allows you to assign specific parameters for how an application will run for users or groups on the network or on local machines. The parameters set for a user or group will apply each time that user or group launches the application. Application launch parameters set for an individual take precedence over parameters set for a group or for an application. When a client launches an application through GO-Global, the Program Window will first check for launch parameters assigned to the individual user. If no parameters are assigned, it will check the list of Groups the user belongs to, in the order the Program Window obtains them from the system. Otherwise, the Program Window will look for generic launch parameters assigned to the application.

Tip: Check the user's ***About GraphOn GO-Global*** box to verify what Group or Groups the user is assigned to and in what order the Groups are listed in the system.

File permissions for users and groups are controlled by Windows NT file system (NTFS) security settings on the host. File permission are *not* set through the Cluster Manager. When you select an application from the Installed Applications list, the Application Users/Groups list displays the user permissions that have been specified for that file and/or application with NTFS. You can then edit the application's properties for specific users or groups. File permissions can only be set on drives formatted with NTFS. If you are using the FAT file system, you will be unable to set permissions for specific files or restrict access to applications.

To assign application launch parameters for a user or group

1. Click the **Applications** tab.
2. Select an application from the list of **Installed Applications**.
3. Select a user or group from the **Application Users**/**Groups** list.
4. Click the **Properties** button.
5. Do any of the following:
   - In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
   - In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
   - In the **Command-Line Options** box, type the command-line arguments you want to use when launching the application.

Note: If you are using the FAT file system, you cannot set permissions for specific files or restrict access to applications.

Removing Applications

GO-Global-deployed applications are removed through the Cluster Manager. Removing an application from the Cluster Manager does not uninstall it from the host; it only prevents GO-Global clients from accessing the application.

To remove an application

1. Click the **Applications** tab.
2. From the Installed Applications list, select the application(s) you want to remove.
3. Click the **Remove** button.

   –or–

   Click Tools | Applications | Remove.

If you remove an installed application from the Cluster Manager while a user is running the application, the user's session is not interrupted. When the user exits that application, however, the application will no longer be available, and the icon will not appear in the Program Window.

Managing Sessions and Processes

Administrators can encrypt and shadow sessions and terminate processes and sessions through the Cluster Manager, as described below.

Terminating a Session

When terminating a user's session, all GO-Global-deployed applications that the user is running will be terminated, and the user will be logged off the GO-Global Host.

To terminate a session

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to terminate.
3. Click Tools | Sessions | Terminate.

Ending a Process

A process is any action taking place on a GO-Global Host that is initiated by a client. A client running an application, for example, is a process. Each running application is assigned a unique name and process ID in the Windows Task Manager. These process names and IDs are duplicated in the Cluster Manager. Administrators can end any process from the Cluster Manager.

To end a process

1. Click the **Processes** tab.
2. Select the process or processes you would like to end.
3. Click Tools | Processes | Terminate.

Note: Terminating a session or ending a process without giving users a chance to close their application can result in the loss of data.

Shadowing a Session

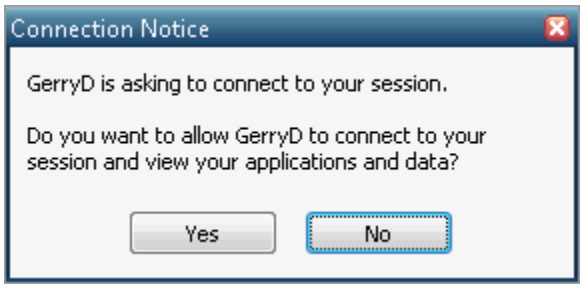
Session shadowing allows multiple users to view and control a single session and its applications. This allows technical support and system administrators to provide remote assistance to customers and users. Session shadowing may also be used for live collaboration.

Only administrators can connect to running GO-Global sessions, but only with permission from the session's user.

To shadow a session

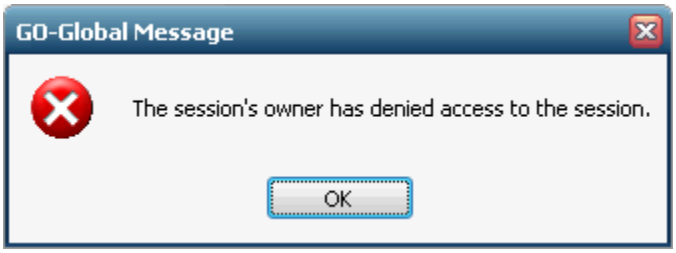
1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to shadow.
3. Click Tools | Sessions | Connect.
   –or–
   From the **Sessions Name** column, right-click the session you would like to shadow.

Once the session is selected, a message such as the following is displayed to the session's user, where GerryD is the administrator's user name:


Connection Notice
GerryD is asking to connect to your session.
Do you want to allow GerryD to connect to your session and view your applications and data?
Yes
No

If the user clicks **Yes** and permits access to his or her session, the connection is made immediately and the GO-Global client session opens in a new frame window.

If the user clicks **No** and denies access, the following message is displayed on the host:



Session shadowing will also be denied when the session is disconnected, when the session is about to be or is in the process of being shut down, or when the user fails to respond within one minute. Connection is also denied in the event of a GO-Global communication failure.

The **Sessions** tab of the Cluster Manager displays the number of clients connected to a session. 2 or higher in the **Connected Clients** column indicates that the session is being shadowed. Disconnected sessions have 0 connected clients. To disconnect from a session and end session shadowing, simply close the frame window where the session is displayed.

Note: When a GO-Global session is being shadowed, the host's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

Security Options

Through the **Security** tab of the **Host Options** dialog, administrators can select the transport mode of communication between clients and the GO-Global Host and select the level of encryption for data transmitted between client and host. Administrators can also modify the host port setting and enable Integrated Windows authentication and password caching.

Selecting SSL Transport

GO-Global provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between Windows and GO-Global Hosts. When selecting the SSL transport, an SSL Certificate file must be specified. SSL certificates are required to secure communication between GO-Global clients and hosts. You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. Wildcard SSL certificates are also supported.

Obtaining a Trusted Server Certificate

To obtain a server certificate from a CA that is trusted by the client operating system, consult the documentation from the CA of your choice using the following information as a guide. The CA will require a Certificate Signing Request (CSR).

To generate a CSR

1. Download **OpenSSL** from http://www.openssl.org/related/binaries.html. (Please note that you must install the *full* version of OpenSSL: Win32OpenSSL-v0.9.8a.exe.)
2. Install **OpenSSL** on the GO-Global Host.
3. Click Start | Run.
4. Type **cmd**, and press **Enter**.
5. Type the following command to generate a private key for the server:
   `[OPENSSL_DIR]\bin\openssl genrsa –out server.key 1024` where `OPENSSL_DIR` is the path to the directory in which OpenSSL is installed (e.g., C:\OpenSSL).
6. Type the following command:
   `[OPENSSL_DIR]\bin\openssl req –new –key server.key –out server.csr`

Running this command will prompt you for the attributes to be included in your certificate, as follows:

Country Name: US

State: your state

Locality: your city

Organization: your company name

Organizational Unit: your department

Common Name: your server's name

E-mail Address: your e-mail address

Unless you are using a wildcard SSL Certificate, the Common Name *must* match the host name of the GO-Global Host (i.e., the name that users will specify when connecting to the host). Any variation in the name will cause the client to issue a warning when connecting. The output of the above command will be a file named server.csr, which can be sent to your CA. Since GO-Global's SSL implementation is based on the OpenSSL toolkit, the tools used are the same as those used in other OpenSSL-based products, such as the Apache mod_ssl package. Follow instructions provided by your CA for the mod_ssl package to obtain a certificate for your server.

When your CA sends you the signed server certificate file, save it as **server.crt**. Copy this file and the **server.key** file (generated in step 5 above) to a directory on the GO-Global Host that can be accessed from the System account and accounts that belong to the Administrator group but that cannot be accessed from normal user accounts. Finally, select the signed certificate file in the Cluster Manager, as described below.

To select the server certificate

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, select **SSL**.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

Using an Intermediary SSL Certificate with GO-Global

When using an intermediary SSL certificate with GO-Global, you must concatenate your existing certificate with the intermediary certificate. The following example uses the Go Daddy intermediary certificate.

1. Take the .crt and .key files that are being used on the GO-Global Host.
2. Download the Go Daddy intermediary certificate (e.g., GODaddyCA.crt). This should have come with the original certificate purchase but can also be located at the following Go Daddy site: https://certs.godaddy.com/Repository.go
3. Concatenate your .crt and the intermediary .crt file. (Combine them into a third file as follows: copy test_server.crt+GODaddyCA.crt server.crt.)
4. Rename the key file from step 1 to server.key so that it matches the newly created server.crt file.
5. Copy these two files onto the GO-Global Host (e.g., c:\Data).
6. Launch the Cluster Manager. Click Tools | Host Options. Click the **Security** tab.
7. Change the transport to SSL and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.
8. Browse to the SSL certificate server.crt in c:\data and click **OK**. You should not see an error message at this point if you have .crt and .key files with the same prefix.
9. Enable **Notify users when connections are secure** for testing purposes.
10. Click **OK**.
11. Start a GO-Global session from a different system.

Creating Your Own Certificate Authority

Sites with many GO-Global Hosts can create their own certificate authority, then sign each server's certificate from this authority and install the certificate authority certificates onto each client. This will prevent any warnings about untrusted authorities, without requiring the site to obtain a third-party certificate for each server.

There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperate with the OpenSSL toolkit. These tools should be able to generate signed server certificates for use with GO-Global without modification.

A certificate authority is a virtual organization that will sign each of your server keys, allowing the client to assert that the server keys are authentic and have not been tampered with.

To establish the certificate authority, a CA key and self-signed certificate must be created. Once the CA certificate and key are created, import the CA certificate on the client device via the Internet Options dialog. Finally, the server keys are signed using the CA certificate, which will allow the client machines to recognize the authenticity of the signatures and allow connections to the server without warning the user about the trustworthiness of the CA.

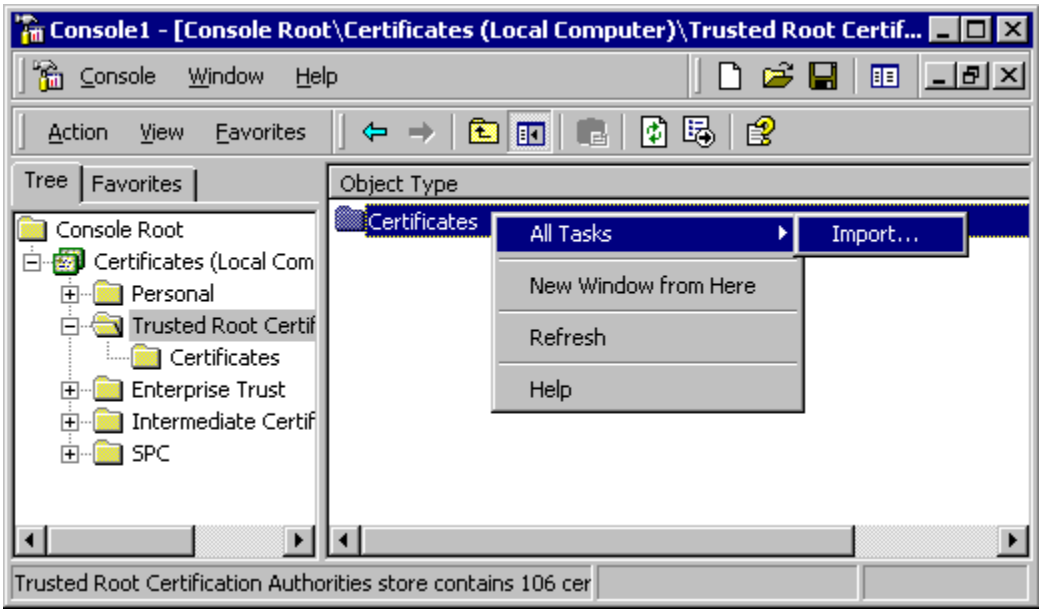
Note: Nine files are created during this process: ca.key, ca.csr, ca.crt, ca.cfg, ca.serial, server.cfg, server.key, server.crt, and server.csr.

Importing the Trusted Server Certificate on a Dependent Host

To import the trusted server certificate on a dependent host, add a Policy in Microsoft Management Console. This is only required when using a self-generated certificate.

1. On the dependent host, click Start | Run. Type **mmc** in the **Open** box. This will open Microsoft Management Console.
2. Click Console | Add/Remove Snap-in. Click **Add**.
3. Click **Certificates** from the list of **Available Standalone Snap-ins** and click **Add**.
4. Select Computer account in the **Certificate Snap-in** dialog. Click **Next**.
5. In the **Select Computer** dialog, select Local computer. Click Finish.
6. Close the **Add Standalone Snap-in** dialog.

7. Return to the **Add/Remove Snap-in** dialog and click **Certificates (Local Computer)**.
8. Click **Ok**.
9. Under **Console Root**, expand **Certificates**. Click **Trusted Root Certification Authorities**. From the right pane, right-click **Certificates**.
10. Select All Tasks | Import. Browse for the Certificate **ca.cert**.



The server key and certificate files (e.g., server.key and server.crt) must have the same base filename and be located in the same directory on the GO-Global Host. Dependent hosts do not need SSL certificates, but their designated relay server must have a valid SSL certificate that is signed by a CA and that is recognized by the dependent hosts. You can verify that these conditions are met as follows:

1. Run the native Windows Client on the dependent host:
2. Right-click **My Compute**r.
3. Click **Explore**.
4. Browse to the \GO-Global\Programs directory.
5. Double-click **gg-client.exe**.
6. Enter the name of the relay server as it is specified in the Cluster Manager.
7. If the relay server has a valid SSL certificate that is signed by a CA and is recognized by the dependent host, no **Security Alert** dialog will be displayed. If a **Security Alert** dialog is displayed, the dependent host will not be able to connect to the relay server.

Creating a CA Key and Certificate

The first step to establishing a certificate authority (CA) is to generate an RSA private key. This key should be kept very secret, as any entity with access to this key can generate false certificates that would certify unknown hosts as trusted. It is vitally important to protect the integrity of your certificate authority. To generate the CA key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa -out ca.key 1024
```

This command will generate your initial CA key, and place it in the file ca.key. After the key is created, generate a Certificate Signing Request (CSR) that will be used to create the CA certificate. To generate the CSR, use the following command:

```
[OPENSSL_DIR]\bin\openssl req -new -key ca.key -out ca.csr
```

This command will run interactively and prompt you for the information to be contained in the certificate. Example responses are shown below:

Country Name (2 letter code) [AU]:*US*

State or Province Name (full name) [Some-State]:*Washington*

Locality Name (e.g., city) []:*Bellevue*

Organization Name (e.g., company) [Internet Widgits Pty Ltd]:*GraphOn Corporation*

Organizational Unit Name (e.g., section) []:*GraphOn Corporation CA*

Common Name (e.g., YOUR name) []:*GraphOn Corporation CA*

Email Address []:hostmaster@graphon.com

Please enter the following *extra* attributes to be sent with your certificate request:

A challenge password []:*[enter]*

An optional company name []:*[enter]*

The prompts should be answered as:

Country Name: your two-letter country abbreviation

State or Province Name: your full state or province name

Locality Name: your city or town or suburb name

Organization Name: the name of your organization or company

Organizational Unit Name: the organizational name should be a representation of your CA's name

Common Name: This should either be a person responsible for the operation of the CA or a generic name representing the CA itself

Email Address: This should be an e-mail address that can be used to address concerns about certificates to someone responsible for the CA

The final step is establishing the CA certificate. To do this, create a settings file that contains some information about the CA. The file should be named **ca.cfg** and should contain the following:

```
extensions = x509v3
[ x509v3 ]
subjectAltName  = email:copy
basicConstraints = CA:true,pathlen:0
nsComment = "[your company] site CA"
nsCertType = sslCA
```

After creating this file, you can sign your CA certificate with the following commands:

```
OPENSSL_DIR]\bin\openssl x509 -req -extfile ca.cfg -days 1825 -signkey ca.key -
in ca.csr -out ca.crt
```

The resulting certificate file, **ca.crt**, is the certificate that will need to be imported into the certificate store on each client device. It is also necessary to create a configuration file for signing server keys. This file should be named **server.cfg**, and should contain the following:

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
nsComment = "Certificate signed by your company CA"
nsCertType = server
```

You must also create a file that will store the serial numbers of certificates signed by this CA. Use the following command:

```
echo 01 > ca.serial
```

Creating and Signing Server Keys

To create a new server key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa –out server.key 1024
```

This will generate a new server key and place it in the file **server.key**. Next, generate a Certificate Signing Request (CSR) for the server key. This is essentially the same process used for generating the CSR for the CA key, but the inputs are slightly different. Use the following command:

```
[OPENSSL_DIR]\bin\openssl req –new –key server.key –out server.csr
```

This command will run interactively and prompt you for information about the server certificate that will be generated. Example input is shown below:

Country Name (2 letter code) [AU]:*US*

State or Province Name (full name) [Some-State]:*Washington*

Locality Name (eg, city) []:*Bellevue*

Organization Name (eg, company) [Internet Widgits Pty Ltd]:*Company Name*

Organizational Unit Name (eg, section) []: *Engineering*

Common Name []:*server*

Email Address []:user@company.com

Please enter the following 'extra' attributes to be sent with your certificate request:

A challenge password []: *[enter]*

An optional company name []: *[enter]*

Your answers to these prompts should be:

Country Name: Your 2-letter country abbreviation

State or Province Name: Your full state or province name

Locality Name: The city, town, or suburb where your organization is located

Organization Name: The name of your company or organization

Organizational Unit Name: Either a department name or some name representing this server

Common Name: The name of this server, as it should appear on the certificate. Note that this is not the name of a person.

Email address: The e-mail address of a party responsible for this server

The Common Name *must* match the host name of the GO-Global Host. Any variation in the name will cause the client to issue a warning when connecting.

Finally, sign the server's key with the CA's certificate. Use the following command:

```
[OPENSSL_DIR]\bin\openssl x509 –req –extfile server.cfg –days 1825 –CA ca.crt
–CAkey ca.key –CAserial ca.serial –in server.csr –out server.crt
```

Note that the -days 1825 parameter will cause our server certificates to expire in 1825 days, or roughly 5 years. If you want certificates to expire earlier or later, adjust this number to fit your requirements.

Copy the **ca.crt**, **server.key** and **server.crt** files to a directory on the target server that can be accessed from the System account but cannot be accessed from the accounts of users who will sign in to the host. Finally, select the server certificate in the Cluster Manager.

To select the server certificate

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, select SSL.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

Your GO-Global Host now has a new SSL certificate, signed by your own custom certificate authority.

Generating a CSR Using IIS Certificate Wizard

The following example uses Microsoft's **IIS Certificate Wizard** to generate a Certificate Signing Request (CSR), and then uses OpenSSL to generate the certificate. In this example, the administrator is the CA.

In order for this certificate to work in GO-Global a private key is required. When you generate a CSR with the IIS Certificate Wizard, a private key is created but it is not presented to the user by default. As a result, the private key needs to be backed up separately using the MMC (Microsoft Management Console). For instructions, see http://www.thawte.com/ssl-digital-certificates/technical-support/backup.html, and look under the Microsoft IIS 6.0 heading.

The private key in this case is a .pfx file, not a .key file, and it must be converted to PEM format in order to work with GO-Global. Use the following command to convert the pfx file to the PEM format:

```
openssl pkcs12 -nocerts -in server.pfx -out server.pem -nodes
```

Change the extension of the file from .pem to .key. The resulting file is called **server.key** and is required for SSL to work in GO-Global. It must have the same file prefix as the certificate generated by the CA (i.e., server.crt).

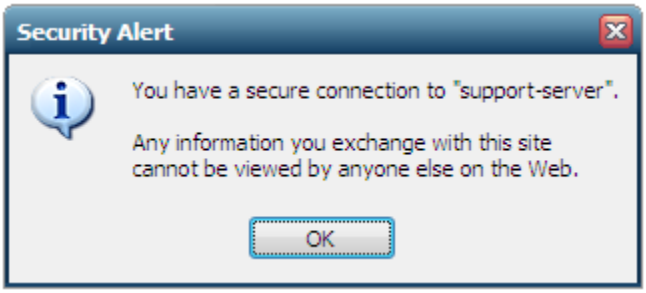
GO-Global requires that the certificate be in PEM format. When requesting a Certificate from a third-party CA, we recommend requesting a certificate in PEM format. If this is not possible and the certificate can only be delivered in DER format, it can be converted to PEM using the following command:

```
openssl x509 -inform der -in MYCERT.cer -out MYCERT.pem
```

The resulting **MYCERT.pem** file can then be renamed to **MYCERT.crt** for use in GO-Global.

Notifying Users of a Secure Connection

When the SSL transport is selected, you can opt to notify users with a Security Alert when connections are secure.


Security Alert
You have a secure connection to "support-server".
Any information you exchange with this site cannot be viewed by anyone else on the Web.
OK

To notify users when connections are secure

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, click SSL.
4. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
5. Click the **Notify users when connections are secure** option.
6. Click **OK**.

When the SSL transport is selected, all connections to that GO-Global Host use the SSL transport and the selected encryption algorithm, including connections from Cluster Managers, clients, and Dependent Hosts.

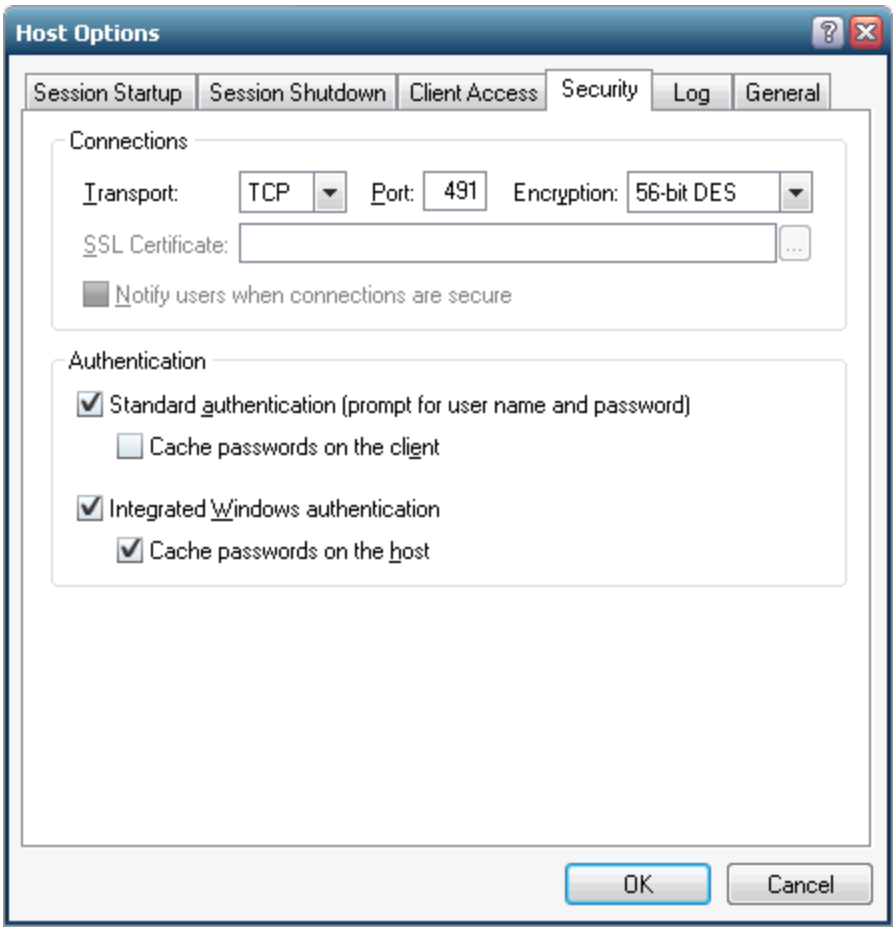
Encrypting Sessions

For purposes of security, administrators can optionally encrypt all data transmitted between the client and the host. This includes the client's user name and password, which are supplied during logon, and any application data submitted by the client or returned by the host. When TCP transport mode is selected, GO-Global uses **56-bit DES** encryption. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits. When SSL transport mode is selected, the following encryption algorithms are also available: **128-bit RC4**, **168-bit 3DES,** and **256-bit AES**. A special license is required to use these algorithms. To obtain this license, contact your GO-Global sales representative.

To encrypt a host's sessions

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. From the **Encryption** list, select an encryption level.
4. Click **OK**.

Once you have enabled encryption, all succeeding GO-Global sessions will be encrypted. Sessions that are active when the feature is enabled will remain unencrypted. The next time the user signs in to the GO-Global Host, however, his or her session will be encrypted. The user must sign off the GO-Global Host, and sign back in for his or her session to be encrypted.



Modifying the Host Port Setting

In order for users to access GO-Global through a firewall or router, administrators are able to modify the host port setting for the Application Publishing Service. The Application Publishing Service must be running on a dedicated port. Conflicts may arise if another service is running on the same port. The default port number for both TCP and SSL is 491.

To modify the Host Port setting

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Security** tab.
4. Type a new port number in the **Port** box.
5. Click **OK**.

Once you have modified the host port setting, you will need to modify the **port** parameter from the GO-Global hyperlink. Use the port parameter followed by the new port number. For example, http://hostname/goglobal/logon.html?port=1667

Users running GO-Global from a shortcut will need to append the -hp argument (followed by the new port number) to the shortcut. For example, "C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" -h server1 -hp 1667.

Users can also specify the port number in the **Connection** dialog when signing in to GO-Global. In the **Host Address** box, type the host name or IP address, followed by a colon and the port number. For example, server1:1667. If it's an IPv6 address, the IP address of the host must be in brackets. For example, [fe80::29c:29ff:fe95:519a]:491.

If the new port number is not specified by either of these methods, users will be unable to sign in to GO-Global.

Note: After changing the host port, you must restart the **Print Spooler Service** and the **GO-Global Application Publishing Service** in order for client printing to work on a port other than the default port 491.

Standard Authentication

Standard authentication is the default method for authenticating users on a GO-Global Host. Standard authentication allows users to sign in to GO-Global via the **Sign In** dialog by supplying their user name and password. Once authenticated, users are added to the host's INTERACTIVE group and given the same access rights as if they had signed in to the host at its console.

To enable Standard authentication

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. Click **Standard authentication (prompt for user name and password)**.
4. Click **OK**.

Integrated Windows Authentication

Integrated Windows authentication allows users to connect to a GO-Global Host and start a session without having to sign in to the host and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, GO-Global simply runs the user's session in the same security context as the GO-Global Client. Users are added to the host's NETWORK group instead of its INTERACTIVE group. As a result, they may be denied access to some resources.

When users connect to a GO-Global Host using Integrated Windows authentication, they are able to access most of the same resources on the host that they would be able to access if they signed in to the host interactively. However, depending on the authentication protocols supported by the client's and host's operating systems and the network, when users access resources that reside on other computers on the network they might be required to re-enter their user name and password. If network resources are unable to request a user name and password, access might be denied.

In order to access other computers on the network, the Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported by Windows 2000 or later on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. Windows NT Domains do not support delegation. When Integrated Windows authentication is enabled in this environment, users might not have access to resources that reside on other computers on the network. To avoid these resource access limitations, see **Configuration Requirements for Delegation Support** in Chapter 6.

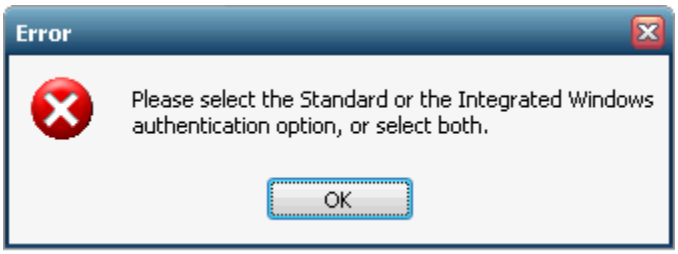
Note: The **Cache passwords on the host** option, described in the following section, can be enabled to obtain an INTERACTIVE group logon with Integrated Windows Authentication.

Integrated Windows authentication is available to users who sign in from Windows computers that are members of the same domain as the GO-Global Host and to users who sign in from Windows computers that are members of Trusted Domains of the GO-Global Host.

To enable Integrated Windows Authentication

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Click **OK**.

GO-Global requires that either Standard authentication or Integrated Windows authentication be enabled. If neither one of these authentication methods is selected and you click **OK** to close the dialog, the following error message is displayed:



If both Standard authentication *and* Integrated Windows authentication are enabled, the GO-Global Host will first attempt to log the user on via Integrated Windows authentication. If this fails, GO-Global will then attempt to log the user on with Standard authentication by presenting the **Sign In** dialog and requiring a user name and password.

Password Caching on the Host

When a user signs in to a GO-Global Host with standard authentication (either with a user name and password supplied by the **Sign In** dialog, parameters, or command-line arguments), that user is added to the host's INTERACTIVE group. Alternatively, a user that signs in to a GO-Global Host using integrated Windows authentication is added to the host's NETWORK group. By default, members of the INTERACTIVE group have greater access to the host's resources than members of the NETWORK group. As a result, a user that signs in via Integrated Windows authentication may encounter "access denied" errors under a number of conditions.

Note:	Areas restricted from members of the NETWORK group include DCOM (also known as OLE and COM/COM+) security limitations, file security limitations, and application specific security checking. Administrators should verify that all resources (files, services, etc.) that Integrated Windows authenticated users need to access have the proper security settings to allow that access.

To avoid these errors, administrators can enable the **Cache passwords on the host** option. Doing so allows users to sign in from Windows computers that are members of the same domain as the GO-Global Host without having to enter their user name and password every time they connect. Users are prompted for a password when first connecting to the host or following a password change. Passwords are stored within their respective profiles and can only be decrypted from within their respective security contexts. With subsequent connections to GO-Global, users are automatically signed in and added to the host's INTERACTIVE group. They are granted the same access rights had they signed in to the host at its console.

Caching passwords on the host requires delegation, which is supported by Windows 2000 or later on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. For

a list of configuration requirements for delegation see **Configuration Requirements for Delegation Support** in Chapter 6.

To enable password caching on the host

1. From the Cluster Manager click Tools | Host Options.
2. Click the **Security** tab.
3. Enable **Integrated Windows authentication**.
4. Enable **Cache passwords on the host**.
5. Click **OK**.

GO-Global caches passwords on the host using the industry standard encryption algorithms provided by Microsoft's Data Protection application programming interface (DPAPI). For more information about DPAPI search the MSDN Library (http://msdn.microsoft.com/library/default.asp) for "Windows Data Protection."

Password Caching on the Client

Client-side password caching allows users who are not members of the GO-Global Host's domain to sign in to GO-Global without having to enter their user name and password every time they connect to the server. When **Cache password on the client** is enabled, the **Sign In** dialog includes a **Remember me on this computer** checkbox. If the user enables this, after the first manual authentication, the user's logon credentials are encrypted on the host, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the server, the cached password is transmitted back to the host, where it is decrypted. The **Sign In** dialog is displayed with the user name and password and with **Remember me on this computer** checked. If the user disables the **Remember me on this computer** option, the user's credentials will be deleted from the client computer.

GO-Global caches passwords on the client using an RSA algorithm with a 512-bit key that is stored on the host. The encryption key is stored in the %ALLUSERSPROFILE%\GraphOn\ks\ks.dat file. Only members of the host's Administrators group and the SYSTEM account can read this file.

Note: In clusters of GO-Global hosts, the key file from one host needs to be copied to *all hosts* in the cluster.

To enable client-side password caching

1. From the Cluster Manager click Tools | Host Options.
2. Click the **Security** tab.
3. Enable **Standard authentication (prompt user for user name and password)**.
4. Enable **Cache passwords on the client**.
5. Click **OK**.

On most platforms, the cached password is stored in the user's home directory in a .dat file named for the GO-Global Host. With the Pocket PC Client and the Windows CE Client, the cached password is stored in the user's Registry settings. The table below provides example locations of the cached password for each GO-Global Client. In the examples, user1 is the user name, server1 is the name of the GO-Global Host, and 192.168.100.111 is the IP Address of the GO-Global Host.

Platform	Password Locations
Mac OS X	/Users/user1/.gg-client/192.168.100.111.dat
Windows	C:\Documents and Settings\user1\Application Data\GraphOn\GO-Global\server1.dat
Linux	/home/user1/.gg-client/192.168.100.111.dat
Pocket PC	In the Registry: KEY_CURRENT_USER\\Software\\Graphon\\GO-Global\\Client\CachedPasswordServers\\SERVERNAME
Windows CE	In the Registry: HKEY_CURRENT_USER\\Software\\Graphon\\GO-Global\\Client\CachedPasswordServers\\SERVERNAME

Client-side password caching is supported on all GO-Global clients.

Password Change

Users can change passwords when:

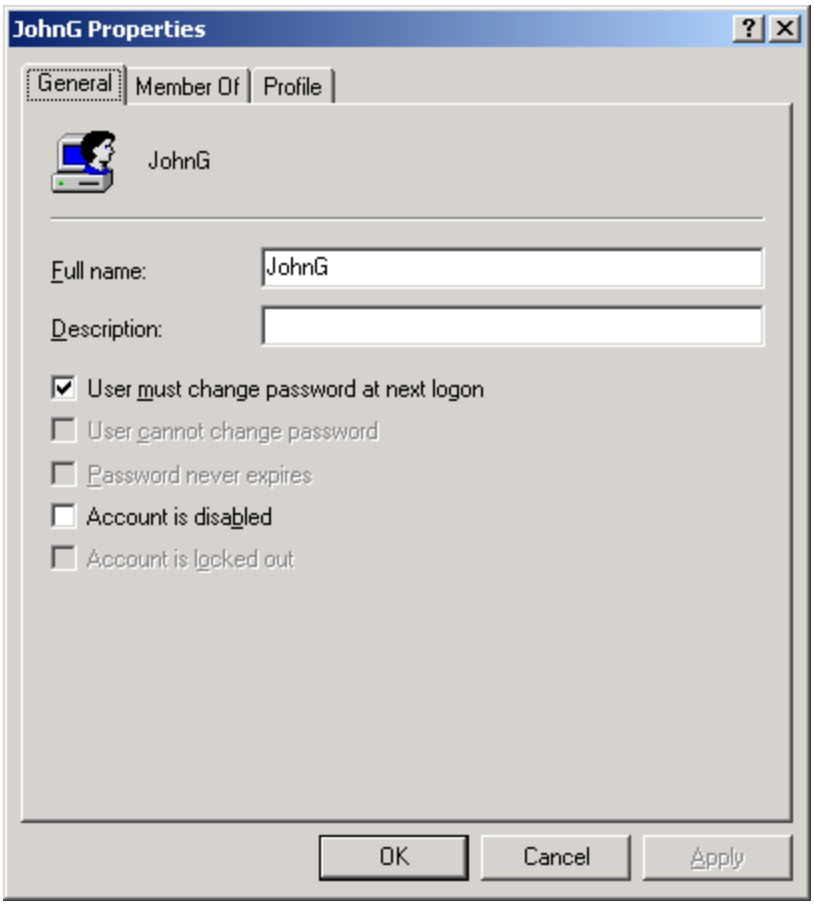
a. The administrator requires the user to change his or her password at the next logon;
b. The security policy is configured to prompt users to change passwords before expiration; and
c. The user's password has expired.

Changing Passwords at Next Logon

Administrators can require a user to change his or her password by checking the **User must change password at next logon** option in the **Administrator Properties** dialog. (For Local accounts, this dialog can be accessed by clicking My Computer | Manage | Local Users and Groups | Users | *UserName* | Properties).

To sign in when the *User must change password at next logon* option is enabled for a user's account

1. Access the GO-Global client installation file (e.g., http://host/goglobal/clients.html) and select a GO-Global client.
2. Type the user name and password in the **Sign In** dialog. If the client account does not exist in the domain in which the GO-Global Host resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message: "You are required to change your password at first logon."
5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change password** dialog.
6. Click **OK**.



Prompting Users to Change Passwords Before Expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password "prompt" period by editing the Prompt user to change password security setting. For example, the local security setting can be viewed and changed by clicking Start | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Option.

To log on during the password change "prompt" period

1. Access the GO-Global client installation file (e.g., http://host/goglobal/clients.html) and select a GO-Global client.
2. Type the user name and password in the **Sign In** dialog.
3. Click **OK**.
4. The following message is displayed:
   "Your password will expire in x day(s). Do you want to change your password now? Yes/No"
   If the user clicks **No**, the GO-Global session will start. If **Yes**, the **Change Password** dialog is displayed.
5. Type a new password in the **New Password** and **Confirm New Password** fields.

Prompting Users to Change Passwords After Expiration

To log on after a password has expired

1. Access the GO-Global client installation file (e.g., http://host/goglobal/clients.html) and select the appropriate GO-Global client.
2. Type the user name and password in the **Sign In** dialog. If the client account does not exist in the domain in which the GO-Global Host resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message: "Your password has expired and must be changed."
5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change Password** dialog.
6. Click **OK**.

Password Change and Integrated Windows Authentication

When Integrated Windows Authentication is enabled, GO-Global relies on the operating system of the client to change passwords. For example, GO-Global supports the following scenario:

1. The administrator edits a user's settings and specifies that the **User must change password at next logon**.
2. Upon logging on, the user is prompted to change his or her password.
3. The user changes the password and signs in to the client computer.
4. The user starts the GO-Global client and connects to a GO-Global Host.
5. The password has already been changed, so the user is authenticated on the host without being prompted for a password, unless the **Cache passwords on the host** option is enabled. In this case, the user will be prompted to enter a new password.

If, however, the administrator specifies that the **User must change password at next logon** after the user has logged on to the client computer, and the user subsequently connects to a GO-Global Host that has Integrated Windows authentication enabled, authentication may fail. If it fails and both the **Integrated Windows authentication** and **Cache passwords on the host** option are enabled, the user will be prompted to sign in and make a password change as described above.

Note: In the Cluster Manager's dialog boxes, you can easily get Help by right-clicking an item, and then clicking **What's This?**. A pop-up window will appear, displaying a brief explanation of the item. You can also get Help by clicking on the title bar of a dialog box and then selecting an item.

Session Reconnect

Session reconnect allows sessions to be maintained on a GO-Global Host without a client connection. If the client's connection to the host is lost, intentionally or unintentionally, the user's session and applications remain running on the GO-Global Host for the length of the session timeout specified in the Cluster Manager. Session reconnect allows users to return to their GO-Global session in the exact state they left it. Through the Program Window users can select to disconnect, rather than exit from GO-Global, and can return to their session as they left it — without having to shut down their open applications and running processes.

If the network connection is lost or if users unintentionally disconnect from GO-Global, their session state is preserved for the length of time specified in the Cluster Manager. After a user is authenticated through normal logon procedures, GO-Global determines if the user has an active session. If so, that session resumes and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials. After the host validates them, the host reconnects them to the disconnected session. If the

session is hosted on a server that is part of a load-balanced configuration, the user is routed to his or her session without any indication that the session is on a load-balanced server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

Setting the Session Termination Option

Administrators control how long client sessions and applications remain running on the GO-Global Host through the Cluster Manager's **Host Options** dialog. Select **Immediately** if you want client sessions to terminate as soon as the client disconnects. Select **Never** if you want sessions to terminate only when a user manually closes all applications running within a session or when an administrator manually terminates a session using the Cluster Manager. This is the default setting. Select **After __ minutes** to specify the number of minutes that a session will remain running after a client has disconnected from the session. Type the number of minutes in the edit field that a session should remain running after the client disconnects.

The **Sessions** tab of the Cluster Manager displays the number of clients connected to a session. Disconnected sessions have 0 connected clients.

To set the session termination option

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Enable **Disconnected sessions terminate**.
4. Select one of the following session termination options:
   Immediately
   Never
   After ____ minutes. In the edit box, type the number of minutes sessions should remain running after their clients disconnect.
5. Click **OK**.

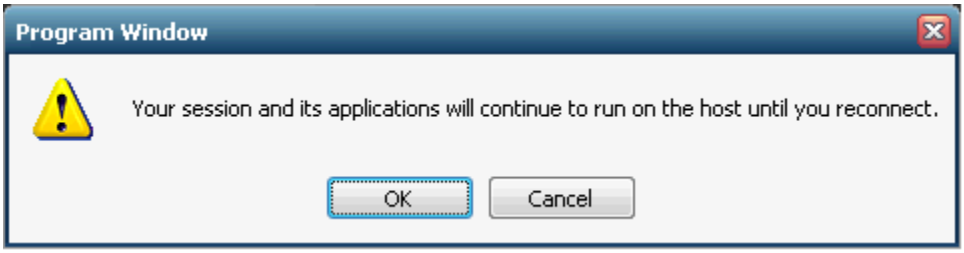
Disconnecting a Session

If sessions are set to never terminate or to terminate after a specified number of minutes, the Program Window's File menu includes a **Disconnect** option. If sessions are set to terminate immediately, the Disconnect option does not appear in the Program Window's File menu.

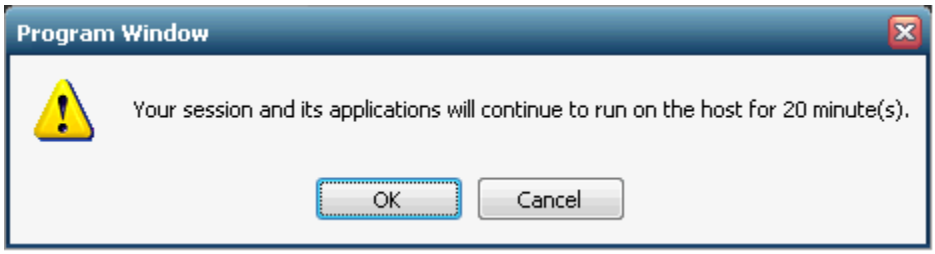
To disconnect a session

From the Program Window, click File | Disconnect.

With session termination set to **Never**, the following message is presented to the user upon disconnecting from GO-Global:



When sessions are set to terminate after a specified number of minutes (20 minutes, for example) a message such as the following is presented to the user upon disconnecting from GO-Global:



If a user attempts to disconnect from a session and already has a disconnected session, the following message appears:

> *You already have a session (session_name) that is disconnected. If you disconnect the current session, that previous session will be terminated.*
> *Do you want to continue?*

If the user clicks **Yes**, the disconnected session is terminated. If **No**, the user is returned to the running session.

Note: When a user reconnects to a session, the command-line arguments -a, -r, and -ac are ignored.

Shared Account

A shared account should be specified when multiple users are using the same account for starting a GO-Global session. Users who sign in to GO-Global with a shared account cannot disconnect and then reconnect to GO-Global. This prevents a user from reconnecting to another user's session.

When logging on to a GO-Global Host with a shared account, the **Disconnected sessions terminate** option in the Cluster Manager is ignored, and the behavior is determined by the *SessionTimeoutBrokenConnection* property in the **HostProperties.xml** file. (HostProperties.xml is located in C:\Documents and Settings\All Users\Application Data\GraphOn on Windows XP and Windows 2003; and in C:\ProgramData\GraphOn on Windows Vista, Windows 2008 and later). If the value of this property is set to 0, the session will terminate immediately. If the value is greater than zero, the session will be suspended and will remain running on the server for the number of minutes specified. In the latter case, only the user who started the session will be able to reconnect to the suspended session. By default, SessionTimeoutBrokenConnection is set to 4320 minutes.

To specify a shared account

1. Click Tools | Host Options.
2. Click the **General** tab.
3. Type the user name of the shared account in the **Shared account** edit box. If multiple shared accounts are required, separate the user names of the accounts with semicolons.
4. Click **OK**.

If an administrator designates an existing user name as a shared account while that user is disconnected from his or her session, the session will remain running on the server until the termination limit has been reached. The session will then be terminated. Before specifying a shared account, verify in the Cluster Manager that there are no connected or disconnected sessions using that account.

GO-Global does not support the use of domain names (for example, NORTH\johng) for shared accounts.

Client Time Zone

By default, all GO-Global sessions are run in the time zone of the GO-Global Host machine. Administrators can opt to run GO-Global sessions in the time zone of the client computer by enabling the **Use client's time zone** option from the Cluster Manager.

To enable client time zone

1. Click Tools | Host Options.
2. Click the **General** tab.
3. Enable **Use client's time zone**.
4. Click **OK**.

Monitoring Host Activity

The Cluster Manager displays information about host activity and processes taking place on the host. Administrators can use this information to determine which applications are no longer being used and whether additional hosts are required, for example.

Viewing Session Information

The Cluster Manager displays the following session information:

Column	Displays the...
Session Name	Unique identifier assigned to a session.
User	Network user name of the user accessing applications on the host.
Connected Clients	Number of clients connected to a session. 0 indicates that no one is connected to the session (the client has disconnected). 1 indicates that the client is connected and the session is active. 2 or higher indicates that the session is being shadowed.
IP Address	IP address of the client computer from which the user is accessing the host. (Each computer on a network has a unique IP address.)
Startup Time	Date and time the user started the application.
Applications	Number of applications the user is accessing.

To view session information
Click the **Sessions** tab.

Viewing Process Information

A process refers to the specific application that a user is running from the host. The Cluster Manager displays the following process information:

Column	Displays the...
Name	Name of the application running on the host.
User	Network user name of the user accessing the application.
Startup Time	Date and time the user started the application.
Process ID	Process identification number assigned by the host's operating system. (The number for each running application matches the process identification number displayed in the Windows Task Manager.)

To view process information

Click the **Processes** tab.

Refreshing the Cluster Manager

You can manually update the sessions, processes, and applications information displayed in the Cluster Manager or you can set it to update automatically. If the Cluster Manager is set to update automatically, you can still update it manually at any time.

To refresh the Cluster Manager

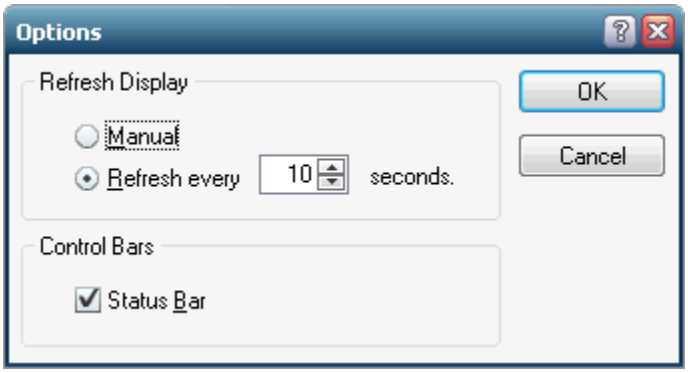
Click View | Refresh.

Setting the Refresh Rate

You can set the sessions, processes, and applications tabs of the Cluster Manager to manually refresh or to automatically refresh at a specified frequency.

To set the refresh rate to allow only manual refresh

1. Click View | Options.
2. Click **Manual**.



To set the refresh rate to refresh automatically

1. Click View | Options.
2. Click the **Refresh every *x* seconds** option.
3. Type a value in the **seconds** box.

The Status Bar

The Status Bar is displayed at the bottom of the Cluster Manager window. The Status Bar provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The Status Bar indicates the name of the GO-Global Host currently being accessed, as well as the Mem usage and CPU utilization for that host, as calculated by the Windows Task Manager. The last two items on the Status Bar, Sessions and Procs indicate the number of sessions and the number of processes running on the active GO-Global Host.

If **All Hosts** is selected, the **Sessions** number will reflect all the sessions running on the network, and the **Procs** number will reflect all the processes on the network.

To turn the Status Bar on or off

1. Click View | Options.
2. Select or clear the **Status Bar** check box.

Setting the Broadcast Interval

You can modify how often host information is sent to the Cluster Manager by modifying the Broadcast Interval value. This value represents how many milliseconds elapse between broadcasts, affecting how often a host's CPU, MEM, Sessions, and Processes status bars are updated, and how long it will take a host to appear in the list of **All Hosts**. The broadcast is sent via UDP and has a packet size of approximately 25-37 bytes.

To set the broadcast interval

1. Stop the **GO-Global Application Publishing** Service.
2. Locate the file **HostProperties.xml** in one of the following directories: C:\Documents and Settings\All Users\Application Data\GraphOn (On Windows XP and Windows 2003); C:\ProgramData\GraphOn (On Windows Vista, Windows 2008 and later).
3. Open **HostProperties.xml** in Wordpad and locate the following section:
```
</property>
<property id="BroadcastInterval" group="Miscellaneous" type="UINT32">
<value>300</value>
</property>
```
4. Type the desired number of milliseconds for the value. (This value must be an integer greater than or equal to 1. Setting the value to 0 will prevent other GO-Global Hosts from being listed in the Cluster Manager. The default value for Broadcast Interval is 300.)
4. Start the **GO-Global Application Publishing** Service.

Session Startup Options

Through the **Session Startup** tab of the Cluster Manager's **Host Options** dialog, administrators can enable startup options such as Group Policy, Progress Messages, and Logon Scripts. Administrators can also set various resource limits.

Applying Group Policy

GO-Global supports Microsoft's Group Policy. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options. For more information regarding this feature, go to: http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx.

To apply Group Policy on a GO-Global Host

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Apply Group Policy**.
4. Click **OK**.

Note: It may take users longer to sign in to GO-Global when Group Policy is enabled.

Displaying Progress Messages

After a user is authenticated, a dialog that reports session startup progress can be displayed to users. When enabled, these messages inform users of the following:

- When their personal setting are being loaded
- When Group Policy is being applied
- When network drives are being connected
- When logon scripts are being run

To display session startup progress messages to users

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Display progress messages**.
4. To ensure that messages are displayed in front of all other windows, select **Always in front**.
5. Click **OK**.

Note: If a logon script has the ability to display user interface to the user, the **Always in front** option should not be enabled. Otherwise, the logon script's user interface may be partially obscured by the progress message.

Logon Scripts

Logon scripts allow administrators to configure the operating environment for GO-Global users. Scripts may perform an arbitrary set of tasks such as defining user-specific environment variables and drive letter mappings.

GO-Global supports two types of logon scripts: global scripts that execute for all users that sign in to the host, and user-specific scripts that execute for individual users. Before loading the user's profile and launching the Program Window, GO-Global's Logon Manager checks to see if a script of either (or both) type has been specified. If so, the Logon Manager runs the script(s) within the user's security context each time the user is authenticated.

User-specific logon scripts are specified using the functionality provided by the operating system. For example, the logon script for local users on a Windows Server 2003 is specified as follows:

1. Right-click **My Computer** and click **Manage**.
2. Navigate to \System Tools\Local Users and Groups\Users.
3. Select a user and click **Properties**.
4. Click Profiles.
5. In the **Logon script** box, type the file name of the user's logon script.

If the value entered in the **Logon Script** box specifies a file name and extension only, GO-Global searches for the file in the following directories, in the following order:

1. If the user's account is a domain account:
    a. *pdcname*\NETLOGON, i.e., the NETLOGON share of the primary domain controller.

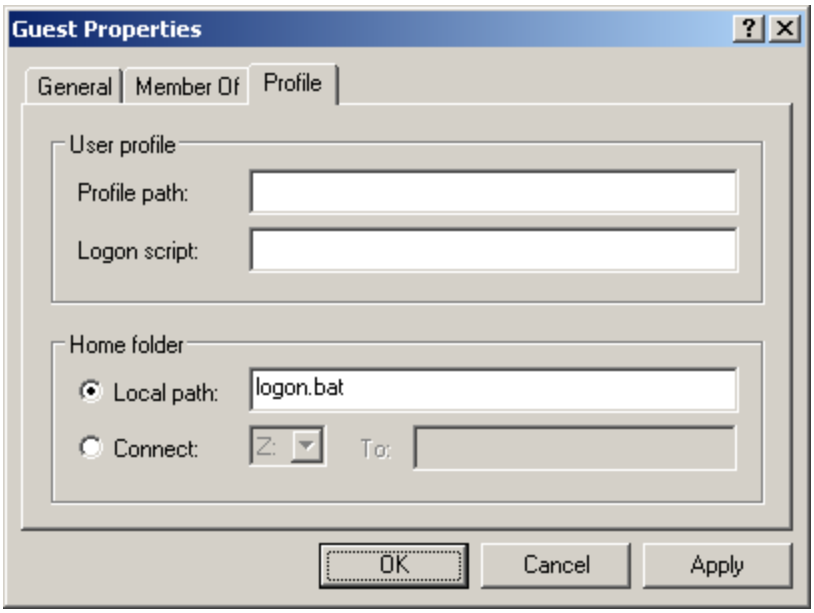
    b. *pdcname*\SYSVOL*domainname*, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.

2. If the user's account is a local account:

a. *systemroot*\System32\Repl\Import\Scripts

b. *systemroot*\sysvol\sysvol*domainname*

If the logon script is stored in a subdirectory of one of the above directories, precede the file name with the relative path of that subdirectory. For example, Admins\JohnG.bat.



Administrators specify global and user-specific logon scripts through the Cluster Manager's **Session Startup** dialog.

To run user-specific logon scripts

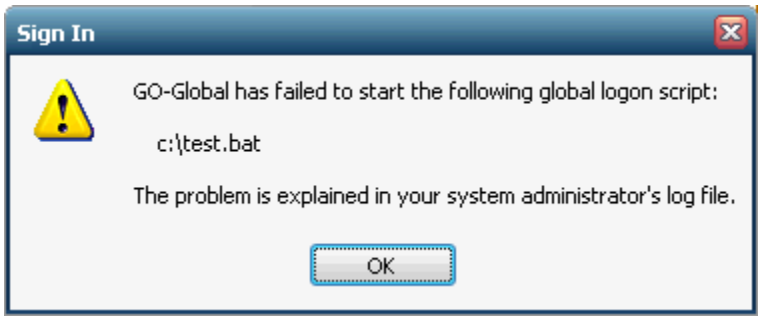
1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **User-specific**.
4. Click **OK**.

To run a global logon script

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Global** and specify the path of the global script file.
4. Click **OK**.

Note: Authenticated users must have read and execute access to the logon script files.

When a logon script fails to execute, an error message such as the following will be displayed:


Sign In
GO-Global has failed to start the following global logon script:
c:\test.bat
The problem is explained in your system administrator's log file.
OK

When such an error occurs, check the location of the logon script. If the user's account is a **domain** account:

a. *pdcname*\NETLOGON, i.e., the NETLOGON share of the primary domain controller.

b. *pdcname*\SYSVOL*domainname*, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.

If the user's account is a **local** account:

a. *systemroot*\System32\Repl\Import\Scripts

b. *systemroot*\sysvol\sysvol*domainname*

Additional tools such as DebugView, available from http://www.microsoft.com/technet/sysinternals/utilities/DebugView.mspx can help track the cause of the problem when these errors occur. Open the DebugView executable on the host and check for any errors that point to the incorrect location of the script.

Note: Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.

Setting Resource Limits

GO-Global allows administrators to prevent users from starting new sessions when certain resource limits are exceeded on a GO-Global Host. These limits help administrators prevent hosts from becoming loaded to the point where users experience performance problems and random resource allocation failures.

To limit the number of sessions per user

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Startup**.
3. Select **Maximum sessions per user** and enter the maximum number of sessions per user in the edit box.
4. Click **OK**.

Specifying the Maximum Number of Sessions

The maximum number of sessions that can be supported from a given host is set to 50 by default. Administrators should adjust this value to one that is appropriate for the capacity of the host.

To edit the maximum number of sessions per host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Session Startup** tab.
4. Edit the number in the **Maximum sessions on this host** box. This will set the limit for the number of sessions the host can support. For example, if the maximum number of sessions is 11, the user who initiates the twelfth session will be prevented from logging on.
5. Click **OK**.

In a relay server setting, GO-Global checks the maximum sessions setting on the relay server and its dependent hosts. The **Maximum sessions on this host** value designated on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server.

Specifying the Minimum Physical and Virtual Memory

To prevent users from logging on when the available physical memory on a host falls below a given value, enter the value in the **Minimum available physical memory** edit box.

To prevent users from logging on when the available virtual memory on a host falls below a given value, enter the value in the **Minimum available virtual memory** edit box.

Session Shutdown Options

Through the Cluster Manager, administrators can specify time limits for the number of minutes of client idle time and the number of minutes that sessions are allowed to run on a host. Administrators can also specify whether the user is either disconnected or logged off when the idle limit is reached, and when to display warning messages to users about to be disconnected or logged off. Administrators can also designate a grace period during the log off period to allow users to save files and close applications, etc.

Specifying the Session Limit

The session limit is the number of minutes that a session is allowed to run on a GO-Global Host.

To specify the session limit

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Enable **Session**.
4. In the edit box, type the number of minutes that a session is allowed to run on a host before its user is logged off.
5. Click **OK**.

The minimum amount of session time is 1 minute and the maximum is 44640 minutes (31 days). This feature is disabled by default.

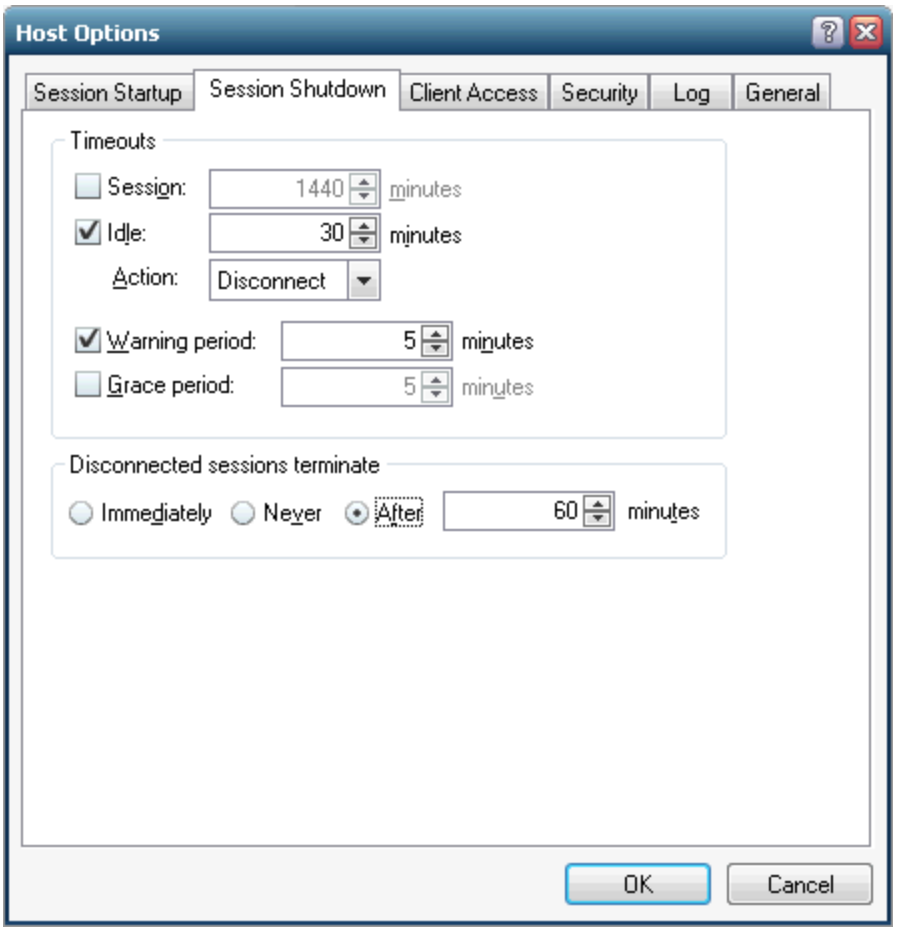
Specifying the Idle Limit

Idle time refers to the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that a GO-Global Host allows.

To specify the idle limit

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Session Shutdown** tab.
3. Enable **Idle**.
4. In the edit box, type the number of minutes of idle time allowed by the host.
5. From the **Action** list, click **Disconnect** to disconnect users when the idle limit has been reached or click **Log off** to log users off when the idle limit has been reached.
6. Click **OK**.

The minimum amount of idle time is 1 minute and the maximum is 44640 minutes (31 days). This feature is disabled by default.



Specifying the Warning Period

The warning period refers to the number of minutes before a session limit or idle limit is reached when users are warned they are about to be disconnected or logged off. For example, if the warning period is set to 2, users will be warned 2 minutes before the session limit or the idle limit is reached. This feature is disabled by default.

To specify the warning period

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Warning period**.
4. In the edit box, type the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off.
5. Click **OK**.

Note: The warning period must be less than the session limit and idle limit settings.

Specifying the Grace Period

The grace period refers to the number of minutes after a logoff begins during which users may save files, close applications, etc. Grace period is enabled and set to one minute by default. The minimum grace period value is one minute and the maximum value is 15.

To specify the grace period

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Grace period**.
4. In the edit box, specify the number of minutes after a logoff begins that users are able to save files and close applications, etc.
5. Click **OK**.

Managing GO-Global Hosts from Client Machines

Administrators can connect to the Cluster Manager from any client machine. This allows the administrator to end processes, terminate sessions, and administer applications from any machine running a GO-Global client.

To access the Cluster Manager from a client machine

1. Set the permissions for the Cluster Manager so that only GO-Global Administrators can access the application.
2. In Windows Explorer, locate cm.exe from the GO-Global\Programs folder.
3. Right-click **cm.exe** and select **Properties**.
4. In the **Properties** dialog box, select **Security**.
5. In the **Security** dialog box, select **Permissions**.
6. In the **File Permission** dialog box, set the permissions so that only GO-Global Administrators can execute the application. (For help with setting permissions in Windows Explorer, choose the Help button from the File Permission box, or press F1 while running Explorer.)
7. Add the Cluster Manager (cm.exe) as a registered application with the Cluster Manager.
8. From the client machine, log on to a GO-Global Host as a GO-Global Administrator, or as a user with administrative rights on the host. This will launch the Program Window.
9. From the Program Window, launch the Cluster Manager by clicking the Cluster Manager icon. (This icon will only appear in the Program Window if the user has administrative rights on the host.) You can administer applications and user access as if running the Cluster Manager from the GO-Global Host.

Keyboard Shortcuts for the Cluster Manager

Action	Result
Applications Tab	
Double-click the application	Displays **Application Properties** dialog
DELETE*	Removes selected application
CTRL+A*	Displays **Application Properties** dialog
CTRL+S	Displays **Application Properties for Users/Groups** dialog
Sessions Tab	
DELETE	Terminates selected session
Processes Tab	
DELETE	Terminates the selected process
General	
CTRL+TAB	Cycles through tabs
CTRL+SHIFT+TAB	Reverse cycles through tabs
CTRL+P	Displays **Options** dialog
CTRL+B	Turns **Status Bar** on or off
ALT+F4	Exits the Cluster Manager
F1	Displays Help for the Cluster Manager
F5	Refreshes the Sessions, Processes, and Applications tabs
INSERT	Displays **Add Application** dialog box

*An application from the list of Installed Applications must be selected in order for these shortcuts to work.

CHAPTER V

Running GO-Global

5

GO-Global can be run from a computer's desktop or from a Web browser.

Running GO-Global from a Computer's Desktop

To run GO-Global from the desktop of a computer, first install the GO-Global Client.

To install the GO-Global Client

1. Start a Web browser (e.g., Mozilla Firefox or Internet Explorer).
2. In the Location box, type http:// followed by the host name and GO-Global client installation page. For example, **http://hostname/goglobal/clients.html**
3. Follow the on-screen instructions which will prompt you to download and run the client setup program for your computer's operating system.

After installing the GO-Global Client, you can run GO-Global from the Start menu, a shortcut, or a console window.

To run GO-Global from the computer's menu

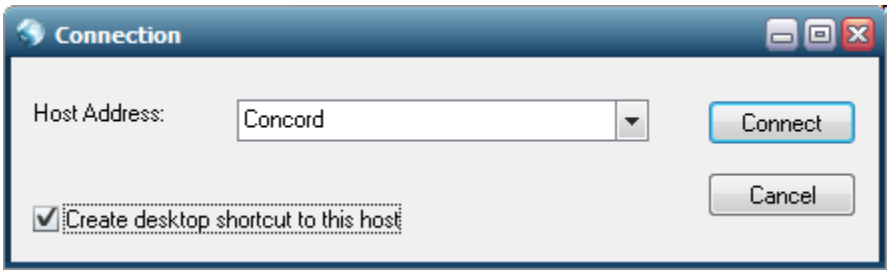
1. Select the GO-Global menu option:
    a. On Windows, click the **Start** button on the Windows taskbar, and select Programs | GraphOn GO-Global 4 | GO-Global.
    b. On Linux, select the Network or Internet category from the Applications menu, then click **GO-Global**.
    c. On Mac OS X, select Go | Applications from the menu, then double-click **gg-client**.
2. Type the address of the host in the **Connection** dialog.
3. Click **Connect**. When the **Sign In** dialog appears, type the following information:
    - Network user name in the **User name** box.
    - Network password in the **Password** box.

Note: GO-Global allows users three invalid logon attempts before shutting down the logon process.

On Windows computers, the GO-Global **Connection** dialog has an option to create a shortcut to a GO-Global host. You can use this option to bypass the **Connection** dialog when connecting to a host.

To create a shortcut to a GO-Global Host on a Windows computer

1. Start GO-Global via one of the above methods.
2. Type the address of the host in the **Connection** dialog.
3. Select the **Create desktop shortcut to this host** check box.
4. Click **Connect**. A shortcut to the host will be created on the desktop of the computer.



In addition to the above methods, you can also run GO-Global from a console window.

To run GO-Global from a console window

1. Open a console window.
2. Type **gg-client**
3. Type the server address in the **Connection** dialog.
4. Click **Connect**.

Running GO-Global from a Web Browser

GO-Global can be run from popular Web browsers, including Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

To run GO-Global from a Web browser

1. Start a Web browser.
2. In the Location box, type http:// followed by the host name and the GO-Global logon page. For example, **http://hostname/goglobal/logon.html**
3. Follow any on-screen instructions that prompt you to install a GO-Global add-on for your browser.
4. When the **Sign In** dialog appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

GO-Global Startup Parameters

GO-Global supports the following shortcut and hyperlink parameters:

Shortcut	Hyperlink	Description
-u	**user**	The name of the user's account.
-p	**password**	The user's password.
-h	**host***	The network name of the GO-Global Host.
-hp	**port**	The port on which the GO-Global Host accepts connections. (491 by default.)
-a	**app**	The application to run. This may be a command-line string or the application name, as registered with the Cluster Manager.
-r	**args**	Application arguments.
-c or -nc	**compression**	-c or compression= "true" enables compression. –nc or compression= "false" disables compression. compression=true by default.
-ac	**printerconfig**	Determines how printers are initialized at startup. When printerconfig ="all" or –ac is followed by **all**, all printers are automatically configured. When printerconfig = "none" or –ac is followed by **none**, printers are not automatically configured. When printerconfig = "default" or –ac is followed by **default**, the default printer is configured automatically. This is the default setting.
-f	**clientframe**	When set respectively to 1 or "true", all applications running in the session will be displayed within a bounding window. When set respectively to 0 or "false", applications will be displayed within their own individual windows.
-geometry		The width and height of the client window. For example: -geometry=800x600
	multimonitor	When set to "true", the session's desktop will span all monitors. When set to "false", applications will be confined to the primary monitor. multimonitor = "true" by default.
	width	The width of the frame or embedded window. 800 by default.
	height	The height of the frame or embedded window. 600 by default.
	newWindow	When set to "true", applications will run in a new browser window. When set to "false", applications run within the existing browser window. newWindow = "false" by default.
	embed	When set to "true" applications run within the browser window. When set to "false" applications run outside the browser window. embed = "true" by default.
	autoclose	When autoclose ="true" closing the Program Window closes the associated browser window and ends the user's GO-Global session. When autoclose ="false", the browser window will remain open after the user's session has ended. autoclose ="false" by default.

	bInBrowser	bInBrowser only applies when the Plug-in is run in loose windows mode. In this mode, when bInBrowser ="true", users will be disconnected from their GO-Global sessions when they close the browser or browse to another page. In these cases, the session will terminate on the host based on the host's timeout settings for disconnected sessions. When bInBrowser ="false", GO-Global will run in a separate process and users will not be disconnected from their sessions when they close the browser or browse to another page. bInBrowser ="false" by default.
	noscale	When noscale is set to "true" and the browser is resized, the resolution of the embedded GO-Global session will adjust accordingly, rather than scaling the displayed image on the client. noscale is set to "false" by default.

*If no host is specified in the logon HTML page, GO-Global detects the machine from where the logon file was downloaded, and makes the connection to that host. The **Connection** dialog is not displayed and the user is presented with the **Sign In** dialog only. If host= "?" users will be prompted for the address of the host.

If an application is not specified, the Program Windows opens.

Note: When autoclose ="true" and bInBrowser ="true," the browser window will close when the user's session ends. When autoclose ="true" and bInBrowser ="false," the browser window will close as soon as the client has started.

To create a GO-Global shortcut on Windows

1. Right-click on the desktop.
2. Click New | Shortcut.
3. In the **Create Shortcut** dialog box, browse to the GO-Global Client executable. For example, "C:\Program Files\GraphOn\GO-Global Client\gg-client.exe"
4. Add parameters after the path to gg-client.exe. For example:

   "C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" –h servername –a Wordpad *–r "C:\Users\Public\Public Documents\test.rtf"*

5. Type a name for the shortcut and click **Finish**.

To use shortcut parameters on Mac OS X

1. Open Terminal.
2. Change to the /Applications/gg-client.app/Contents/MacOS/ directory.
3. Type **./ gg-client** and append command-line arguments.

EXAMPLE: ***./gg-client –h 196.125.101.222 -c -ac all -hp 443***

- Parameters are optional and case-insensitive. They can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last parameter on the command-line and it must be used with the **–a** parameter.
- When the **–a** parameter is used, the Program Window is not launched, even if the application does not exist.
- Startup parameters passed on by the **-r** parameter are specific to each application. Please refer to the application's documentation for information about launch parameters.
- If a user does not have a password, **-p ""** can be used to bypass the **Sign In** dialog, as long as the user name has also been specified in the shortcut.

- Parameters containing spaces must be enclosed in quotation marks. For example, the parameter **–a "Acrobat Reader"** would launch Adobe's Acrobat Reader. Likewise, user name Jim C would be specified as **–u "Jim C"**.

When GO-Global is run from a Web browser, GO-Global startup parameters can be specified by adding arguments to hyperlinks that reference the logon.html page. These hyperlinks can then be inserted into documents, Web pages, e-mails, instant messages, etc.

To create a GO-Global hyperlink

1. Open a Web page in an editor.
2. Choose the editor's **Insert Hyperlink** option.
3. Enter the address of the host, followed by the desired hyperlink parameters. For example:
   http://hostname/logon.html?mode=embed&width=1024&height=768&app=C:\Program%20Files\Windows%20NT\Accessories\wordpad.exe&args=C:\Users\Public\Public%20Documents\test.rtf
4. Save the page.

- Parameters are optional and case-sensitive. They can be appended in any order.
- Spaces within parameters must be replaced with "%20".

Resizing the Client Window

The command-line argument **–geometry** can be used to modify the size of the client window when the command-line argument **–f** is used. Without -geometry on the command-line, the client window will be maximized. When the GO-Global Client is run in loose window mode, -geometry has no effect.

To resize the client window**,** append **–geometry** to the GO-Global Client executable, followed by the desired width and height.

For example, on Windows:
"C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" -f –geometry=800x600

On Mac OS X and Linux:
./gg-client –h 196.125.010.222 –f –geometry=800x600

Uninstalling GO-Global

Instructions for uninstalling GO-Global depend on the platform and browser.

To uninstall the GO-Global Client on Windows

1. Open Control Panel.
2. Double-click **Programs and Features**.
3. Select **GO-Global Client**.
4. Click **Change**.
5. Click **Next**.
6. Select **Remove**.
7. Click **Next**.
8. Click **Remove**.

To uninstall the GO-Global Client on Linux

1. Launch the Linux console.
2. Type **rpm -e gg-client.linux**.

To uninstall the GO-Global Client on Mac OS X

1. Open Terminal.
2. Log on as **root**. (Type **su** and press **Enter**, then provide the root password).
3. Change to the /Applications/gg-client.app/Contents/Utils/ directory.
4. Run the script by typing **./Uninstall.sh**
5. Close Terminal.

To uninstall the GO-Global Client from Firefox

1. Start Mozilla Firefox.
2. Click Tools | Addons.
3. Click **Uninstall** in the GraphOn GO-Global section.
4. Close Mozilla Firefox.

After uninstalling GO-Global, it is recommend that users clear the Firefox browser cache.

To uninstall the Plug-in for Linux

1. Launch the Linux console.
2. Remove the Plug-in by typing:
   rm -rf ~/.mozilla/plugins/libnpg.so ~/.mozilla/plugins/libpbr.so > ~/.mozilla/ gg-client

If you plan to reinstall the Plug-in, we recommend clearing the Firefox browser cache.

To uninstall the GO-Global Client from Internet Explorer

1. Start Internet Explorer.
2. Click Tools | Internet Options | Programs | Manage add-ons.
3. Select **GO-Global 4**.
4. Click **Delete**. If there is no **Delete** button (e.g., with Internet Explorer 8):
   a. Double-click **GO-Global 4**.
   b. Click **More Information**.
   c. Click **Delete**.

If users have difficulty reinstalling and running the ActiveX Control, clear the browser cache. To do this, open Internet Explorer and click Tools | Internet Options. Click the **General** tab and under **Temporary Internet Files**, click **Delete Files**. Users should then check for any conflict directories using a Command Prompt window.

To check for conflict directories

1. Open a Command Prompt window.
2. Type the location of the **Downloaded program files** folder and check for any conflict directories. If any exist, delete them.
3. Close the Command Prompt window.

To uninstall the GO-Global Client from Apple Safari

1. Open Terminal.
2. Log on as **root**. (Type **su** and press **Enter**. Then provide the root password.)
3. Change to the /Applications/gg-client.app/Contents/Utils/ directory.
4. Run the script by typing **./Uninstall.sh**
5. Close Terminal.

Note: If users experience slow scrolling with GO-Global, try disabling the smooth scrolling option on the host. In Internet Explorer, click Tools | Internet Options. Click the **Advanced** tab. In the **Settings** box, under **Browsing**, disable **Use smooth scrolling**.

Automatic Client Updates

Administrators can configure GO-Global to automatically update the GO-Global Client when users connect to a GO-Global Host that is running a newer version.

To enable Automatic client updates

1. Install the GO-Global Client on client computers using the **gg-client.windows.exe** setup program. (The Automatic client update feature is only available for Windows computers.)
2. From the Cluster Manager, click Tools | Host Options.
3. Click the **Client Access** tab.
4. Enable **Automatically update clients**.
5. Click **OK**.

Mac and Linux users can download the updated client file by connecting to the GO-Global client installation page (e.g. http://hostname/goglobal/clients.html) and installing the appropriate client.

Users who have installed the Plug-in with Mozilla Firefox, can update the Plug-in via Firefox's Add-on manager.

To update the Plug-in

1. In Firefox, select Tools | Add-ons
2. Click the **Find Updates** button.
3. Install the update.

When **Automatically update clients** is selected in the Cluster Manager and a user signs in to the host from a Windows computer, GO-Global compares the version of the GO-Global Client installed on the client computer to the version in the Updates directory on the Host. If the files in the Updates directory are newer, GO-Global copies the newer files to a temporary directory on the client computer. Then, when the GO-Global Client closes, the **GO-Global Update Client** service installs the new files so they can be used in subsequent GO-Global sessions. Users will be updated on the screen when the new updates have completed installing.

In summary, a new GO-Global Client will be installed via the update client service when the following conditions are met:

- **Automatically update clients** is enabled in the Cluster Manager.
- The **GO-Global Update Client** service is installed and enabled on the client computer.
- A newer version of the client is available in the Updates directory on the host.
- All of the files in the new version have been downloaded to the client computer.
- The user has signed out of his or her GO-Global Client session.

Notes:

Automatic client updating for users running the ActiveX Control with Internet Explorer 6.0 is not supported.

The default location for the Updates folder is C:\Program Files\GraphOn\GO-Global\Updates which is defined in the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Updates.

Users are not required to perform any upgrade tasks. They can, however, prevent updates from being installed by disabling the GO-Global Update Client service on the client computer.

To disable the GO-Global Update Client service

1. Right-click My **Computer**.
2. Click **Manage**.
3. Click Computer Management | Services and Applications | Services.
4. Select **GO-Global Update Client**.
5. Click **Properties**.
6. Under **Startup type**, select **Disabled**.
7. Click **Stop**.
8. Click **OK**.

Updating the ActiveX Control and the Plug-in

If GO-Global was deployed via a Web browser's Add-on manager, users should launch a Web browser to access a GO-Global Web server. The Web pages will install and update the Web clients as long as the user has sufficient rights to install browser add-ons. If the user does not have sufficient rights to install browser add-ons (for example, if the user is running Internet Explorer and is not an Administrator or Power User), the client should be installed using the GO-Global Client Setup Program.

Users who have installed the Plug-in with Mozilla Firefox can update the Plug-in via Firefox's Add-on manager.

To update the Plug-in

1. In Firefox, select Tools | Add-ons
2. Click the **Find Updates** button.
3. Install the update.

When users running the ActiveX Control connect to a GO-Global Host with an updated client, the ActiveX Control will update automatically, if users have Power User rights.

Note: The Firefox Plug-in update feature does *not* work if you install the native Windows Client. It only works when the Web client has been installed via the Web browser page.

Windows CE Client

To run the Windows CE Client, devices must have TCP/IP as a network protocol. SEH (the C++ Structured Exception Handling component) and RTTI (the Run-Time Type Information component) are required to run GO-Global on a Windows CE device. To determine if these components exist on the device, open **ceconfig.h** found in the Windows folder.

On a Windows CE 4 device, if the following lines:
#define COREDLL_CRT_RTTI 1
#define COREDLL_CRT_CPP_SEH 1
are included in this file, RTTI and SEH are supported.

On a Windows CE 5 device, if the following line:
#define COREDLL_CRT_CPP_EH_AND_RTTI 1
is included in this file, RTTI and SEH are supported.

Installing the Windows CE Client

Once the Windows CE Client has been installed, users can log on to a GO-Global Host from the Start menu, from a desktop shortcut, or directly from the GO-Global executable. The Windows CE install program attempts to delete **GO-Global.CAB** at the end of installation. As such, we recommended setting the GO-Global.CAB file permission to read-only before installing it on the client device.

To install the Windows CE Client

1. Start Internet Explorer.
2. In the Address box, type http:// followed by the host name and GO-Global client installation file. For example, **http://host/goglobal/clients.html**
3. Click the **Windows CE Client** link.
4. Determine which processor your Windows CE device is using and download the appropriate .CAB file (ARMV4, ARMV4I or X86).
5. Double-click the .CAB file.

The Windows CE Client can be installed manually by launching **GO-Global.CAB** from the corresponding CPU folder on the client device. For example, Web\Clients\GO-Global.CAB

Running the Windows CE Client from the Start Menu

Users running CE devices with taskbar support can run the Windows CE Client from the Start menu.

To run GO-Global from the Start menu

1. Click the **Start** button on the Windows taskbar.
2. Select Programs | GraphOn GO-Global 4 | GO-Global Client.
3. Type your host address in the **Connection** dialog.
4. When the **Sign In dialog** appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Running the Windows CE Client from a Shortcut

On Windows CE devices with desktop shortcut support, a Windows shortcut named **GO-Global Client** is created during installation of the Windows CE Client. This shortcut launches the Program Window.

To run the Windows Client from a shortcut

1. Double-click the **GO-Global Client** shortcut.
2. Type your host address in the **Connection** dialog.
3. When the **Sign In dialog** appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Running the Windows CE Client from the GO-Global Executable

Users with CE devices that do not support the shortcut or Start menu launching options can run GO-Global directly from the GO-Global client executable.

To run the Windows CE Client

1. Run **ggw.exe** on the client device.
2. Type the host address in the **Connection** dialog and click **Connect**.
3. When the **Sign In dialog** appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Command-Line Arguments for the Windows CE Client

If a shortcut for gg-client.exe can be created on the CE device's desktop, command-line arguments can be used to expedite the logon process. For example, the command-line arguments -a allows users to directly launch an application. Command-line arguments can also be used to pass on application specific startup parameters and to enable compression.

To run GO-Global using command-line arguments

1. Right-click on a GO-Global shortcut and click **Properties**.
2. In the **Shortcut** tab, place the cursor in the **Target** edit box and append any of the following command-line arguments after the quote (”):

Argument	Description
-h	The GO-Global Host address or host name.
-u	The client’s network user name.
-p	The client’s network password.
-a	The display name of the application to be launched. The application's display name should be identical to the application registered with the Cluster Manager.
-r	Startup parameters for the application
-hp	Modifies the host port setting for the Application Publishing Service.
-c or -nc	-c enables compression. -nc disables compression. (Compression is enabled by default.)

EXAMPLE: ***...\ggw.exe" -h server -u username -p password -c -hp 443***

- Startup parameters passed on by the **-r** argument are specific to each application. Please refer to the application's documentation for information about launch parameters.
- Command-line arguments are optional and case-insensitive. Arguments can be appended in any order, with the exception of **-r**. If **-r** is used, it must be the last argument on the command-line and it must be used with the **-a** argument.
- In order to accommodate spaces in user names, passwords, application display names, or application arguments, quotation marks must be included when using command-line arguments. For example, user name Jim C would be specified as –u "Jim C".

To edit the name or command-line options of a connection

1. In the **Configure** tab of the **Terminal Connection Manager** select the desired connection to modify.
2. Click **Edit**.
3. Optionally make changes to the name and command-line options for this connection.
4. Click **OK**.

To delete a connection

1. In the **Configure** tab of the **Terminal Connection Manager** select the desired connection to delete.
2. Click **Delete**.

To run a GO-Global connection

1. Click the **Connections** tab of the **Terminal Connection Manager**.
2. Select the desired connection to run.
3. Click the **Connect** button.
4. Type your host address in the **Connection** dialog.
5. When the **Sign In dialog** appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Uninstalling the Windows CE Client

To uninstall the Windows CE Client, delete the installation files from the directory on the client device to which you copied them. These files include:

ggw.exe
clipc.dll
cs.dll
dc.dll
filec.dll
pbru.dll
sc.dll
scres.dll
sndc.dll
printc.dll
upc.dll

Pocket PC Client

GO-Global's **Pocket PC Client** is available for Pocket PC 2003 and Windows Mobile 5 for Pocket PC.

Installing the Pocket PC Client

Once the Pocket PC Client has been installed, users can log on to a GO-Global Host from the Start menu or directly from the GO-Global executable.

To install the Pocket PC Client on devices

1. Open a Web browser.
2. In the Address box, type http:// followed by the host name and GO-Global client installation file. For example, **http://host/goglobal/clients.html**
3. Click the **Pocket PC Client** link.
4. Determine which version of Pocket PC is running on your device.
5. Download the appropriate .CAB file (Pocket PC 2003 or Windows Mobile 5 for Pocket PC).
6. Double-click the .CAB file.

You can manually install the Pocket PC Client by launching **GO-Global.CAB** from the corresponding Pocket PC version on the client device. For example, \Program Files\GraphOn\GO-Global\Web\Clients.

Running the Pocket PC Client from the Start Menu

Users can run the **Pocket PC Client** from the taskbar's Start menu.

To run GO-Global from the Start menu

1. Click the **Start** button on the Windows taskbar.
2. Select **GO-Global Client**.
3. Type your host address in the **Connection** dialog.
4. Select the desired screen size and click **Connect**.
5. When the **Sign In** dialog appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Running the Pocket PC Client from the GO-Global Executable

Users with pocket devices can run GO-Global directly from the GO-Global client executable.

To run the Pocket PC Client

1. Run **ggw.exe** on the client device.
2. Type the host address in the **Connection** dialog.
3. Select the desired **screen size** and click **Connect**.
4. When the **Sign In** dialog appears, type the following information:
   - Network user name in the **User name** box.
   - Network password in the **Password** box.

Using the Pocket PC Client

The Pocket PC has several buttons and scrollbars based upon the screen size selected in the **Connection** dialog. If the screen size selected is larger than the actual screen of the Pocket PC device, horizontal and vertical scroll bars will appear on the right and bottom of the GO-Global window. You can manually move these scroll bars to view different portions of the GO-Global screen.

There are 5 pan buttons located at the bottom of the Pocket PC screen. These buttons allow you to quickly scroll to the four corners and center of the GO-Global screen. There are also 4 zoom buttons located at the bottom of the device's screen. These buttons allow you to zoom-in, zoom-out, fit to screen, and view 100%.

Uninstalling the Pocket PC Client

To uninstall the **Pocket PC Client**, delete the installation files from the directory on the client device to which you copied them. These files include:
gg-client.exe
clipc.dll
cs.dll
dc.dll
filec.dll
pbru.dll
sc.dll
scres.dll
sndc.dll

CHAPTER VI

Advanced Topics

6

Load Balancing

Load balancing allows GO-Global sessions to be distributed across multiple hosts. Load balancing is required when the host resource requirements for a deployment exceed the capacity of a single host computer. Load balancing is done automatically and is transparent to the user. GO-Global can also be used with any third party TCP/IP based load-balancing service.

Load Balancing Requirements

- A GO-Global Host must be installed on each of the hosts in the cluster.
- For Web deployment, if the load balancer is balancing connections to both the Web server (e.g., port 80) and the GO-Global Host (e.g., port 491), each of the GO-Global Hosts in the cluster must have a Web server running and the Web server home directory should contain the GO-Global Web files. If the load balancer is only balancing connections to the GO-Global Host, the GO-Global Web files do not need to be located on each GO-Global Host. Web files can be installed on the machine running the Web server.
- If an application saves any user specific settings in the registry, (e.g., Corel WordPerfect, Microsoft Word, etc.) we strongly recommend that users operate with roaming profiles rather than local profiles. Since there is no way of predicting which server the user will actually be logged onto in a balanced server farm, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

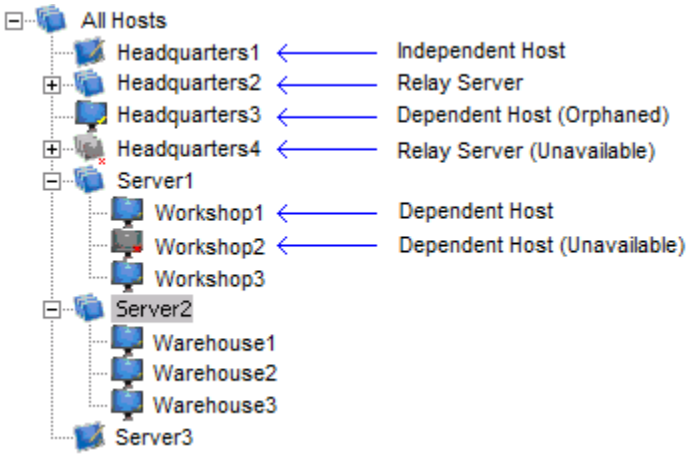
A GO-Global Host can be configured to operate as an independent host, a dependent host, or as a relay server. Please note that a relay server *cannot* be an application host.

When setting up a load-balanced relay server configuration, GraphOn recommends using a license server. For more information, see the following sections from Chapter 2: **Configuring GO-Global to use a Central License Server**, ***Three-Server Redundancy***, and ***License-File List Redundancy***.

Independent Hosts

Independent hosts are GO-Global Hosts that do not interact with other GO-Global Hosts running on the network. Independent hosts appear in the Cluster Manager on the first level of the GO-Global Hosts tree view as an independent node. The GO-Global setup program configures GO-Global Hosts to operate as independent hosts. GO-Global clients can connect to independent hosts directly by specifying the name or IP address of the server in the **Connection** dialog or the location box of a Web browser. Clients can also connect to independent hosts through a third party network load balancer that distributes client connections among several servers. However, session reconnect is not supported in the latter configuration and must be disabled.

GO-Global Hosts



Relay Servers

A relay server is a GO-Global Host that provides centralized control over one or more GO-Global Hosts. Relay servers maintain client connections and distribute GO-Global sessions across a set of load-balanced application hosts. Relay servers appear in the Cluster Manager on the first level of the list of **All Hosts** as nodes with one or more dependent hosts.

To configure a GO-Global Host to operate as a relay server

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **General** tab.
4. Type the name or IP address of the computer in the **Relay server** box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **GO-Global Application Publishing Service** on the relay server has been restarted. Click **OK**.
7. Stop and restart the **GO-Global Application Publishing Service** from the Services option in the Control Panel.

After configuring a host to run as a relay server with one or more dependent hosts, GO-Global load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected host, the relay server selects another host and tries again until it finds one that can support the session.

Notes:

When setting up a relay server environment, be sure the same **Log Folder** path for the relay server exists on the dependent hosts. Otherwise, the **Sign In** dialog will not appear when users attempt to sign in to GO-Global. Create a log directory on the C: drive of each relay server (e.g., C:\Data\APS_LOGS) or use C:\Program Files\GraphOn\GO-Global\Log which already exists on the dependent host.

Make sure this same path exists on the dependent host. In addition to changing the **Log Folder** path in the Cluster Manger, the \Log\Codes and \Log\Templates directories must be copied to the new location.

When a relay server is selected in the Cluster Manager, the number of processes running on all dependent hosts is not listed in the Cluster Manager's status bar.

A relay server requires a minimum of 512 MB of RAM. For most deployments and for best results, 1 GB with a multiprocessor server is recommended. Depending on the number of dependent hosts attached to the relay server, more RAM may be required.

Memory and CPU requirements for the dependent hosts are determined by the applications that are published and the number of users accessing the system. In general, a dependent host can support 12 "heavy" users/500 MHz CPU and 25 "light" users/500 MHz CPU. ("Heavy" is defined as a user running one or more large applications with continuous user interaction. "Light" is defined as a user running one application with intermittent user interaction.)

Dependent Hosts

A dependent host is a GO-Global Host that is connected to a relay server. GO-Global clients cannot connect directly to dependent hosts. Instead, they connect to the associated relay server, and the relay server selects one of the connected servers to host the session.

To configure a GO-Global Host to operate as a dependent host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **General** tab.
4. Type the name or IP address of the relay server in **Relay server** edit box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** has been restarted. Click **OK**.
7. Stop and restart the **GO-Global Application Publishing Service** from the Services option in the Control Panel.

When the Application Publishing Service is restarted, the dependent host will appear beneath the relay server in the Cluster Manager's list of GO-Global Hosts. A dependent host with a yellow x indicates that the host has been "orphaned;" in other words, that its relay server has gone down. If a host's icon has a red x, the administrator does not have administrative rights on the host. If the host's icon has a red x and is grayed out, the host is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that host from the Cluster Manager.

Users are authenticated on dependent hosts, not on relay servers. As a result, dependent hosts can be located on a different network than their associated relay server. For example, dependent hosts can be located behind a firewall on an internal, Active Directory network, and the associated relay server can be located in a demilitarized zone (DMZ) that is outside the firewall. If **Integrated Windows authentication** is used, clients and dependent hosts must be located on the same domain, but the relay server can be located on a different domain.

Note: We recommend installing the same set of applications on each dependent host and using the same installation path.

Administering Relay Servers and Dependent Hosts on Different Networks

When a user starts the Cluster Manager on a relay server or a dependent host, the Cluster Manager connects to the relay server and attempts to authenticate the user using Integrated Windows authentication. If the Cluster Manager is running on a dependent host and the associated relay server is located on a different network, a message such as the following is displayed:

Failed to log you on to Server8. This computer (Server4) and Server 8 may be located on different networks. Would you like to log onto Server 8 and administer it remotely?

Clicking **No** will return you to the **All Hosts** node of the Cluster Manager. Clicking **Yes** will initiate a special remote administration session on the relay server as follows:

1. The Cluster Manager on the dependent host starts the GO-Global Client.
2. The client connects to the relay server and starts a session. The **Sign In** dialog is displayed to the user.
3. The user signs in, specifying the user name and password of an account that is a member of the Administrators group on the relay server.
4. The Cluster Manager starts on the relay server. The user can now administer the relay server and all of its dependent hosts.
5. A maximum of two administration sessions can run on the relay server at any given time, regardless of the **Maximum sessions on this host** setting in the Cluster Manager and regardless of license restrictions.

Dependent hosts inherit their list of published applications, server settings, and user settings from the relay server. Applications *must* be installed in the same directory on all dependent hosts. Applications do not need to be installed on the relay server. When a GO-Global Host is connected to a relay server all of its server settings are synchronized with those of the relay server. When any changes are made to the relay server's settings, they are also made to **All Hosts** connected to that relay server. The only settings that are allowed to vary are the maximum number of sessions and the name of the relay server. All other settings in the **Host Options** and **Application Properties** dialogs are grayed out and cannot be modified.

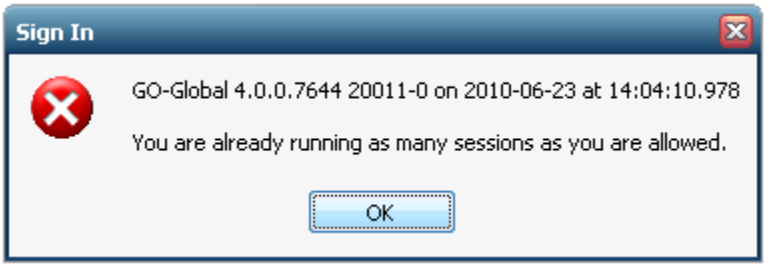
When setting up a relay server, if an application is *installed* but not *published* on the dependent host, you will need to publish the application on the relay server through the Cluster Manager. For example, if Adobe Reader 7.0 is installed on the dependent host at C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe, open the Cluster Manager on the relay server and type this path location in the **Executable Path** box in the **Add Application** dialog.

Note: Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the dependent hosts as it is on the relay server.

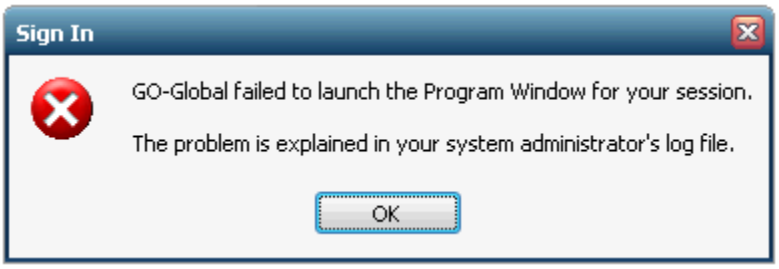
Host Selection

When a client connects to a relay server, the relay server attempts to start a session on the dependent host that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the host.

If the session fails to start on the selected host, the relay server successively attempts to start the session on other available hosts until it finds one that can support the session. If there are no available hosts (i.e., if the number of running sessions on All Hosts equals the maximum number allowed), the following message is displayed to the user:



Otherwise, if the session cannot be started on any of the available hosts, the following message is displayed to the user:


Sign In
GO-Global failed to launch the Program Window for your session.
The problem is explained in your system administrator's log file.
OK

In a relay server setting, GO-Global checks the maximum sessions settings on the relay server and its dependent hosts. The maximum sessions value on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server. To modify the **Maximum sessions on this host** setting, open the Cluster Manager on the host, click Host Options | Session Startup.

Relay Server Failure Recovery

On Windows hosts, the Application Publishing Service can be configured to automatically restart if the service fails. If a relay server fails, clients are disconnected but sessions continue to run on the GO-Global Hosts that were connected to the relay server. These servers will attempt to reconnect to the relay server every 15 seconds. When a dependent host reconnects to the relay server, it re-adds its sessions to the relay server and restores any state information associated with the disconnected sessions. Clients are then able to sign back in and resume their sessions. Clients do not automatically attempt to reconnect to the relay server.

In order to provide higher service availability, a failover server can be configured for the GO-Global relay server using the Microsoft Cluster Service. In this configuration, if the relay server fails for any reason, the failover server immediately takes the place of the failed server. Application hosts automatically reconnect to the failover server, and users will generally be able to log on and reconnect to their disconnected sessions within 1-2 minutes of the relay server failure.

Relay Server in a DMZ

A relay server in a DMZ can be separated from its dependent application servers by a firewall, with the following requirements:

- The dependent application server must be able to connect to the relay server from behind the firewall. Please note that the reverse is *not* required. The relay server does not need to be able to connect to the dependent application server.
- The client must be able to connect to the relay server in the DMZ.

When a session starts on a dependent application server, the dependent application server opens a connection to the relay server. When the relay server receives data from the session's clients, it forwards the data to the session over this connection. Similarly, when the relay server receives data from the session over this connection, it forwards the data to the session's clients.

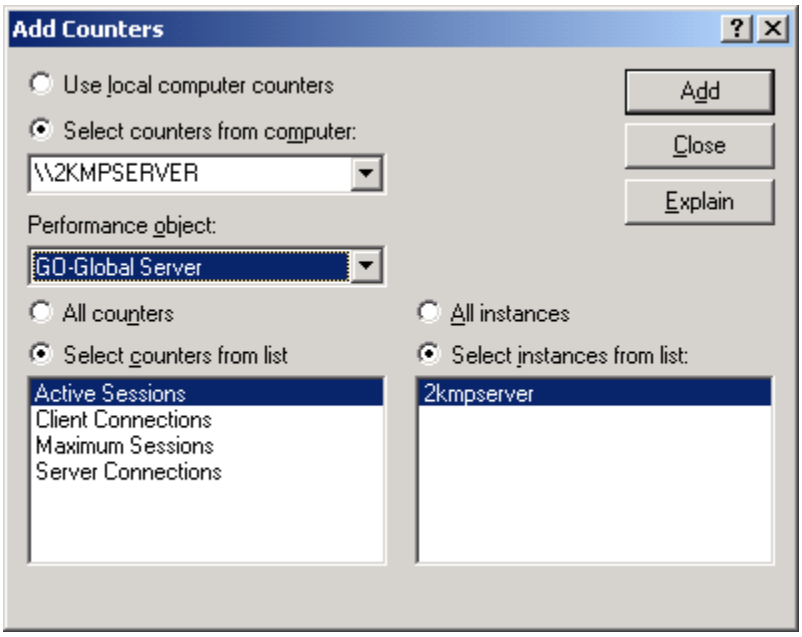
The relay server generally has two network interfaces: one that is accessible from clients outside the DMZ, and one that is accessible from dependent application servers behind the firewall.

GO-Global Host Performance Counters

GO-Global Host performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a host. Performance counters can also be added to track the number of hosts connected to a relay server and to identify the maximum number of sessions allowed on a host. GO-Global Host performance counters allow administrators to monitor host activity from any machine with network access to a GO-Global Host. The Remote Registry Service (Regsvc.exe) must be enabled for remote performance monitoring to work.

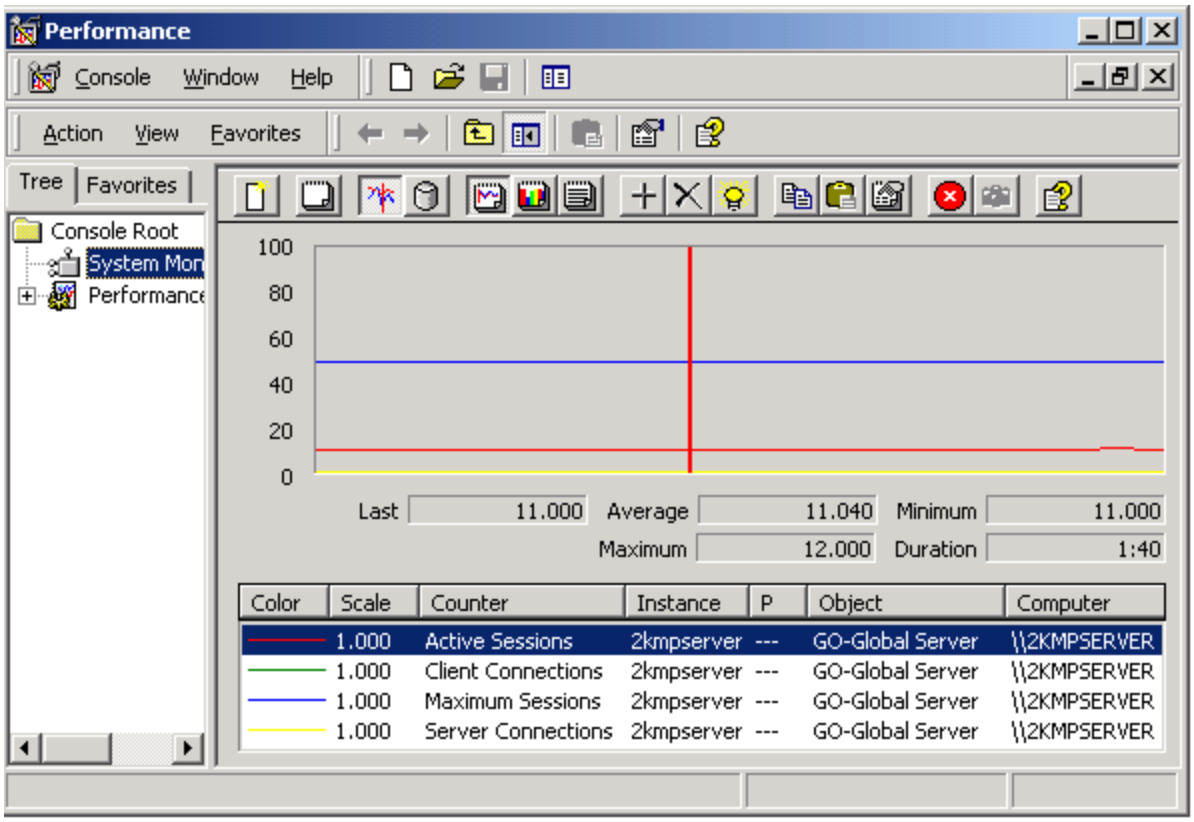
To add GO-Global Host Performance Counters to the Performance Monitor

1. Click Start | Programs | Administrative Tools | Performance.
2. Click the **+** button to add counter(s).
3. From the **Object** field, locate and click **GO-Global Server**.
4. From the **Counter** field, click the desired counters (Active Sessions, Client Connections, Maximum Sessions, Server Connections) and click **Add**.



GO-Global Host Performance Counters include:

- **Client Connections.** The total number of client connections on independent hosts or relay servers. This value is always zero for dependent hosts.
- **Server Connections.** The total number of dependent hosts connected to a relay server. This value is always zero for independent or dependent hosts.
- **Active Sessions.** For independent or dependent hosts this is the number of sessions running on the host. For a relay server this is the total number of sessions hosted on all connected dependent hosts.
- **Maximum Sessions.** This displays the **Maximum Session Count** set in the Cluster Manager's **Host Options** dialog.



Configuration Requirements for Delegation Support

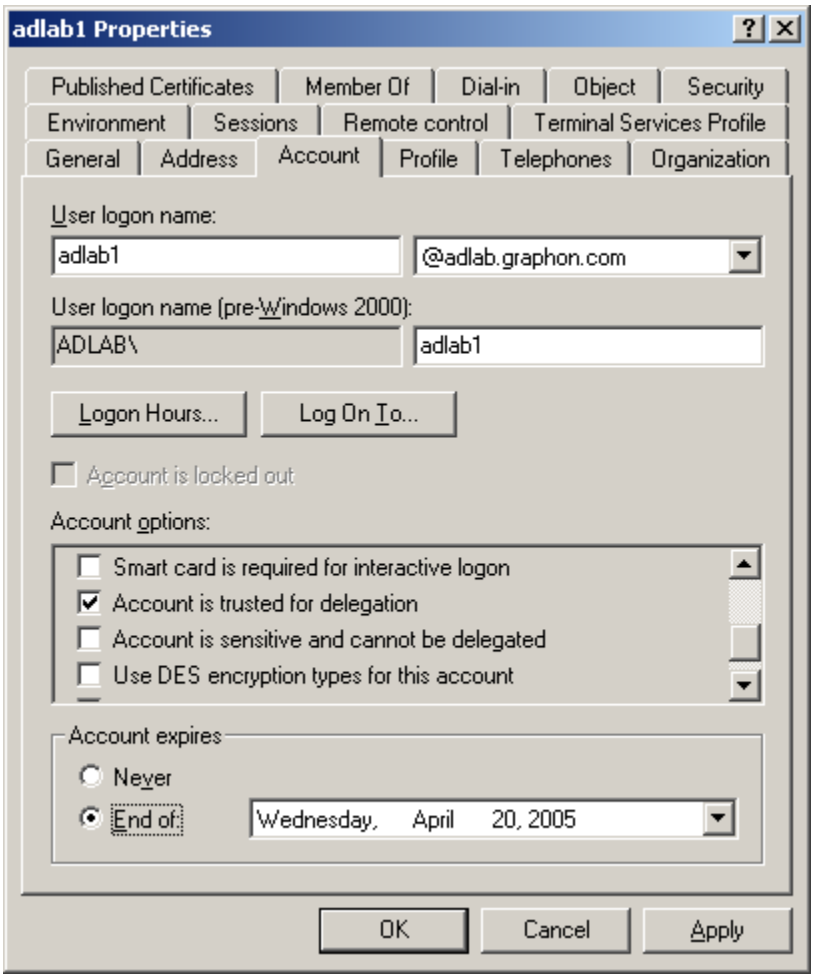
Password caching on the host, as described in Chapter 4, and network resource access require Windows delegation. The configuration requirements for delegation support are as follows:

- Delegation requires the Kerberos authentication protocol and an Active Directory Domain, both of which were introduced with Windows 2000. As such, host-side password caching and accessing shared folders using Integrated Windows authentication are not supported from Windows NT 4.0 or Windows 98 client computers.

- The Domain Name System (DNS) servers must support Service Location (SRV) resource records. It is also recommended that DNS servers provide support for DNS dynamic updates. Without the DNS dynamic update protocol, administrators must manually configure the records created by domain controllers and stored by DNS servers. The DNS service provided with Windows 2000 or later supports both of these requirements.

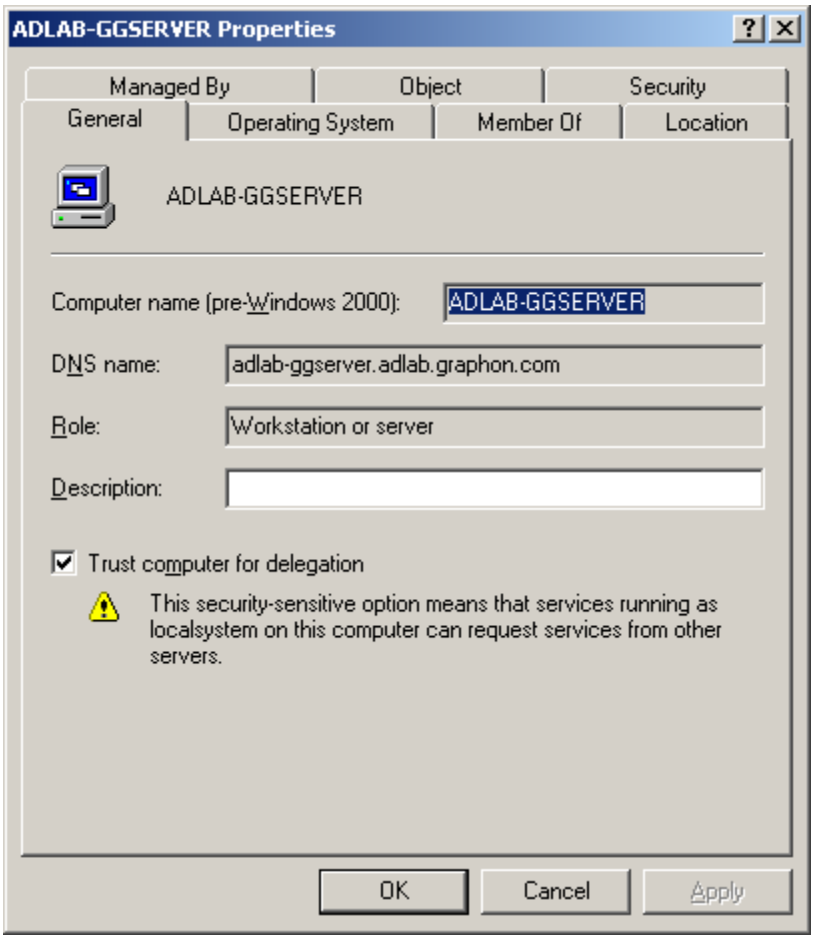
- The computers hosting the GO-Global client, the GO-Global Host, and any backend services, such as email or a database, must support Kerberos. Kerberos is supported by systems running Windows 2000 or later in a Windows 2000 or later Active Directory domain. GO-Global Host is only supported on Windows XP or later.

- The client's user account must support being delegated by the GO-Global Application Publishing Service. In the **Active Directory Users and Computers** Management Console, select the user and click **Action | Properties**. Click the **Account** tab. In the Account options list box, scroll down and ensure the **Account is sensitive and cannot be delegated** option is disabled. Enable the **Account is trusted for delegation** option.

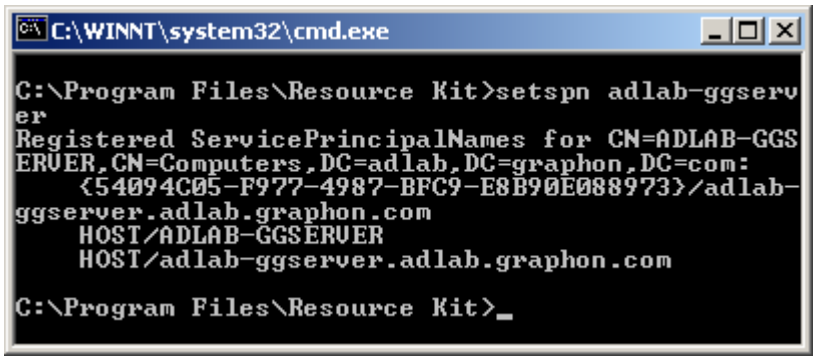


- The GO-Global Host must have the right to delegate the user's account to other computers. In the **Active Directory Users and Computers** Management Console, select the computer and click **Action** | **Properties**. Enable **Trust computer for delegation**. The GO-Global Application Publishing Service must be configured to run in the Local System account for these delegation rights to apply.

Note: After enabling **Trust Computer for delegation** in the Active Directory, the GO-Global Host must be restarted in order for delegation to take effect.

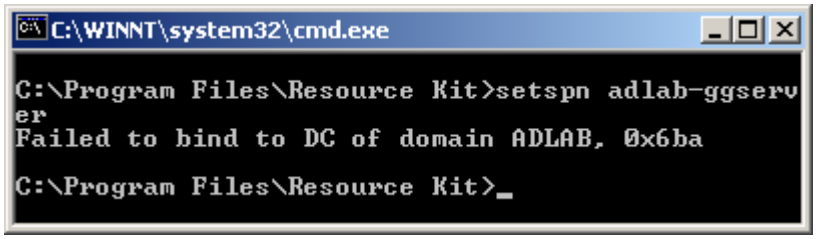


- The **GO-Global Application Publishing Service** must be able to register its Service Principle Name (SPN) with the Active Directory. It attempts to do this every time the service is restarted. The **setspn.exe** utility (available in the Microsoft Resource Kit and as a separate download from Microsoft) can be used to verify the SPN is properly set. The following Command Window shows output obtained from setspn.exe when run on the GO-Global Host.



Replace adlab-ggserver with the computer name of your GO-Global Host. The {54094C05-F977-4987-BFC9-E8B90E088973} Globally Unique Identifier (GUID) is specifically used by the GO-Global Application Publishing Service to create the {54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.graphon.com SPN.

The following Command Window shows output obtained by running **setspn.exe** on the GO-Global Host and indicates a network configuration error. If all the above requirements are met, this should not occur.



Client Printing

GO-Global supports client-side printing on all clients except the Pocket PC Client. By default, GO-Global automatically detects the client's default printer information once the user has signed in to the GO-Global Host. This includes the default printer's port and printer driver. If the printer driver is not installed on the GO-Global Host, GO-Global will attempt to locate the driver and automatically install it.

When running applications on GO-Global Hosts, users can print to network printers and to printers that are directly connected to their computers (e.g., via serial, parallel and USB ports).

Administrators can control which, if any, printers are made available to users using the **-ac** and **printerconfig** GO-Global startup parameters.

When running GO-Global from a shortcut, use the -ac parameter with "all", "none" or "default" to respectively make all, none or only the default printer available from applications running on the GO-Global Host. For example, to make all printers available, create a shortcut with the target specified as follows: "C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" -ac all

Similarly, when running GO-Global from a hyperlink, use the **printerconfig** parameter with "all", "none" or "default". For example, the following hyperlink will make all printers available: http://hostname/goglobal/logon.html?printerconfig=all

If no options are specified, GO-Global automatically configures the user's default printer only.

Note: The **Print Spooler Service** must be running on the GO-Global Host in order to configure client printers.

Designating Access to Printer Drivers

GO-Global can obtain printer drivers from the following sources:

- **Universal Printer Driver**: GO-Global includes a **Universal Printer Driver** that can print to any client printer. Enable this option to allow the use of the Universal Printer Driver for configuring client printers.
- **Windows Printer Drivers:** Enable the **Windows Printer Drivers** option to allow printers to be configured using already installed native drivers. To allow GO-Global to automatically install native printer drivers that ship with Microsoft Windows enable **Automatically install drivers**.

When neither the **Universal Printer Driver** or **Windows Printer Drivers** is enabled, no printers will be configured and client printing is disabled.

When only the **Universal Printer Driver** is enabled, only the Universal Printer Driver will be used as a printer driver. No native drivers will be used. This is the default setting.

When only the **Windows Printer Drivers** option is enabled, only native printer drivers that are installed on the GO-Global Host will be used. If a printer's native driver is not installed, that printer will not be configured. When **Windows Printer Drivers** and **Automatically install drivers** are enabled, only native printer drivers that are installed on the host or those that are included with Windows will be used. If a printer's native driver is not installed and it is not included with Windows, that printer will not be configured.

When both the **Universal Printer Driver** and the **Windows Printer Drivers** are enabled, and a printer's native driver is installed on the host, the printer's native driver will be used to configure the printer. If it is not installed on the host, the printer is configured to use the Universal Printer Driver.

The Universal Printer Driver is supported on Windows, Linux, and Mac OS X. Users running the Windows CE Client must use the Universal Printer Driver. When printing with the Universal Printer Driver, the user (or group) needs to have full access to the temp directory.

A printer named **Preview PDF** is configured in each session when the Universal Printer Driver is enabled. Documents printed to this printer are automatically converted to a .pdf file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe Reader, is required on the client computer in order to use the Universal Printer Driver's PDF conversion feature.

Note: The **Universal Printer Driver** uses a standard printing properties dialog and may not offer some of the more advanced printing options other drivers do.

Administrators set access to printer driver sources through the **Host Options** dialog.

To designate access to printer drivers

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Printers** check box.
5. Click the box beside the desired driver source or sources.
6. Click **OK**.

Client-side printing is enabled by default. Administrators disable client-side printing through the Cluster Manager's **Host Options** dialog.

To disable support for client printers

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Disable **Universal Printer Driver** and **Windows Printer Drivers**. When neither of these options is selected, client printing is disabled.
5. Click **OK**.

Printer Configuration

When GO-Global clients connect to a host, **proxy printers** are automatically created on the host and serve as an interface for printing to the client printer. Proxy printers are printers GO-Global sets up on the host as a bridge between the applications running in a GO-Global session and the client printers. Proxy printers can be configured automatically or manually.

Native printer drivers are preferred when configuring proxy printers — *if* they are available and *if* settings allow them to be used. Alternatively, the **Universal Printer Driver** can be used when the native driver is not available. There are several methods an administrator can use to manage which printer drivers should be used when creating proxy printers. Settings from client printers are replicated in their proxy printer counterpart. A session's proxy printers are removed when the session ends. Proxy printers are not removed when a session disconnects. All proxy printers on the system are removed when the Application Publishing Service starts.

When a proxy printer is configured, there is a hierarchy of preferences when selecting a native printer driver. If the **Windows Printer Drivers** option is disabled in the Cluster Manager, this hierarchy is not applied. Native drivers are selected in the following order:

- **Printers Applet**. A user's manual selection of a printer driver in the Printers Applet takes precedence over all other driver selection methods.
- **Mapped Printer Drivers**. MappedPrinterDrivers.xml contains a list of driver names that can be used for each driver. This file is generated by the Application Publishing Service, but can also be manually edited by administrators.
- **Client driver name**. The driver with the exact name of the driver that is installed on the client is used to configure the proxy printer.

Printers Applet

GO-Global's Printers Applet allows users to add and remove printers, edit printer properties, set the default printer, select a printer driver, and print test pages. The Printers Applet is accessible via the Program Window. It lists all the client printers that are configured and all the host printers that the user has access to. The list of printers depends on the printer drivers setting in the Cluster Manager as well as the –ac and printerconfig parameters.

Icons in the Printers Applet are described below.

	Indicates that the printer is installed on the client
	Indicates the default printer, which is installed on the client
	Indicates the printer is installed on the host
	Indicates the default printer, which is installed on the host

Settings made with the Printers Applet are saved the next time the user signs in to GO-Global. These settings take precedence over command-line options. Printer changes made in the Printers Applet take effect immediately. Users do not need to restart their session.

Adding and Removing Printers

When a printer is added or removed via the Printers Applet, it does not add or remove it from the client computer, it only determines which printers are configured for use with GO-Global.

To add a client printer

1. From the Program Window, click File | Printers.
2. Click the **Add** button.
3. From the **Add Printer** dialog, select the desired printer and click **Add**. This adds the printer to the list of configured printers and is now available for use.

Note: When a printer is added through the Printers Applet, it gets configured at startup regardless of the -ac command-line option or printerconfig parameter.

To remove a printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Remove** button.

Removing a printer from the list prevents it from being configured the next time the user starts a GO-Global session. The printer can be re-added to the list at any time by clicking the **Add** button and selecting it from the list.

Setting the Default Printer

Users can specify their default printer in the Printers Applet. The default printer is indicated by a black circle and checkmark above the printer. Any printer, including host printers, can be designated as the default.

To set the default printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Set Default** button.

Editing Printer Settings

Through the Printers Applet, users can edit printer settings such as layout orientation and paper size.

To edit printer settings

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Edit** button.
4. Edit the properties, as desired, and click **Ok**.

Printing a Test Page

From the Printers Applet, users can print a test page to verify that the printer has been properly configured and to check if a printer is printing graphics and text correctly. A test page also displays information such as the printer name, model, and driver software version, which may be helpful for troubleshooting printer problems.

To print a test page

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Test Page** button.

Changing a Printer's Driver

Through the Printers Applet, users can select different drivers for their printers. This is useful if a driver is not working properly or if a user wants to switch between native drivers and the Universal Printer Driver.

To select a new driver

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Driver** button to open the **Select Printer Driver** dialog, which lists the drivers currently installed on the GO-Global Host machine.
4. Select a new driver, and click **Ok**. The printer is now configured with the new driver.

When only the Universal Printer Driver has been designated as a driver source in the Cluster Manager, users are unable to change drivers. Users cannot change the driver for GO-Global's Preview PDF printer or for server-based printer.

Resetting Printer Settings

At any time, users can reset printer data to its default settings, including preferences and printer settings. This may be useful if printers are not configuring properly or if users are experiencing printer issues.

To reset printer settings

1. From the Program Window, click File | Printers.
2. Click **Reset Printers**.

Resetting printer settings removes all proxy printers from the session. Users must restart their session in order to print to client printers again. This also resets the default printer to its original default setting.

Mapping Printer Drivers

Administrators can map printer drivers by editing MappedPrinterDrivers.xml. For most GO-Global deployments, administrators will not need to edit this file. It is used for specifying which driver to use when a host's driver name does not identically match the client's, or when the administrator wants to override native drivers and force clients to use a different printer driver or the Universal Printer Driver.

To specify a different printer driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn or C:\Documents and Settings\All Users\Application Data\GraphOn.
2. Open the file in Wordpad and search for the client printer driver name, for example,
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```
3. Delete the driver name from the value field. In the example above, delete `HP LaserJet 2100 Series PS` and replace with the desired printer driver.
4. Save the file. This change will take effect the next time the user starts a GO-Global session.

In the example above,
`<property id="HP LaserJet 2100 Series PS" type="STRING">`
is the driver that is used on the client.

`<value>HP LaserJet 2100 Series PS</value>`
is the driver that should be mapped to on the host.

Mappping printer drivers can also be used to force printers to use the Universal Printer Driver.

To force the printer to use the Universal Printer Driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn or C:\Documents and Settings\All Users\Application Data\GraphOn.
2. Open the file in Wordpad and search for the client printer driver name, for example,
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS </value>
   </property>
   ```
3. Delete the driver name from the value field. In the example above, delete `HP LaserJet 2100 Series PS` and replace it with `Universal Remote Printer`, as follows:
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>Universal Remote Printer</value>
   </property>
   ```
4. Save the file.

The next time users connect to the host, their printer will be configured using the Universal Printer Driver.

Multiple drivers can be specified in the <value> field by delimiting them with a semicolon.

To designate an additional driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\GraphOn or C:\Documents and Settings\All Users\Application Data\GraphOn.
2. Open the file in a text editor and search for the client printer driver name, for example,
   ```
   <property id="HP LaserJet 2100 Series PS" type="STRING">
   <value>HP LaserJet 2100 Series PS</value>
   </property>
   ```

3. Specify an additional driver. For example, add HP LaserJet 2100 Series PS to the list, as follows:

```
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2200 Series PS;HP LaserJet 2100 Series PS</value>
</property>
```

4. Save the file.

Administrators can add an unlimited number of driver names to the value. GO-Global attempts to configure client printers using the drivers in the order they are specified. The semicolon-separated drivers specify the preferential order of drivers to be used when installing a proxy printer.

To remove printer driver mapping

1. Open **MappedPrinterDrivers.xml** in a text editor and delete the entire modified line. For example, delete:

```
<property id="HP LaserJet 2100 Series PS" type="STRING">
<value>HP LaserJet 2100 Series PS</value>
</property>
```

2. Save the file.

The **MappedPrinterDrivers.xml** file can be deleted to remove any prior changes. The file is recreated when users sign in to the host.

Notes:

Client printers are temporarily installed on the GO-Global Host for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers in the Printers folder on the GO-Global Host.

To add a default printer for all new users, consult the following article:
http://support.microsoft.com/support/kb/articles/Q252/3/88.ASP

Client Printer Naming Customization

GO-Global installs a printer on the host for each printer that is configured on the client machine. These printers are called proxy printers and are the printers that are seen by users when printing via GO-Global. Since multiple users connect to a GO-Global Host, these printers must be filtered so that users see only their own printers. This requires that each printer be assigned a unique identifier.

Through the Registry, administrators can specify the format of these proxy printer names and include information such as the user's name, the client computer's IP address, and the client machine name. The PrinterNameFormat Registry key is created after a GO-Global session is started.

Administrators can choose from the following tokens to create a suffix to the printer string name:

Token	Description	Example
%U	The user name	Wilson
%I	The client IP address	192.168.100.147
%M	The client's unique ID (GUID)	800fb6b5770-ed9e-11df-82ae-000874b1cdb1
%C	The client machine name	HRWorkstation
%S	The GO-Global session ID	7

To customize the client printer name

1. Run the Registry Editor (regedit.exe)
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the PrinterNameFormat key:
   [HKLM\Software\GraphOn\GO-Global\AppServer\PrinterNameFormat]
4. Right-click **PrinterNameFormat** and select **Modify**.
5. In the **Value data** field, type one or more of the client printer customization tokens.
6. Close the Registry Editor.

The PrinterNameFormat key is set to (from %C) by default. Using the above examples, printer names would appear as: PrinterName (from HRWorkstation)

Any special characters other than % in the PrinterNameFormat string are taken literally, since they are not tokens. There are 12 characters that are not allowed. These characters are ! , \ = / : * ? " < > and |. If any of these characters are used in the string, they are replaced with a hyphen.

Client Clipboard

GO-Global allows client and host-based applications to exchange information using the clipboard. Users can cut and copy information from applications running on the client and paste it into applications running on a GO-Global Host, and vice versa. Clipboard support is disabled by default.

To enable client clipboard

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Clipboard** check box.
5. Click **OK**.

Client Sound

GO-Global supports sound capability for any application that uses PlaySound, sndPlaySound, or waveOut. A sound card must be installed on the host. Speakers are not required on the host. The client machine requires a sound card and speakers. Audio support is disabled by default.

Note: Client Sound requires the loading of GO-Global libraries into session processes. This can affect the startup of a process, make some processes incompatible with GO-Global, or have fatal consequences during suspend/resume operations. For information on advanced configurations options, please consult the **Advanced Session Process Configuration** section in this guide.

To enable audio support

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Sound** check box.
5. Click **OK**.

Client Serial and Parallel Ports

GO-Global allows applications running on the host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default.

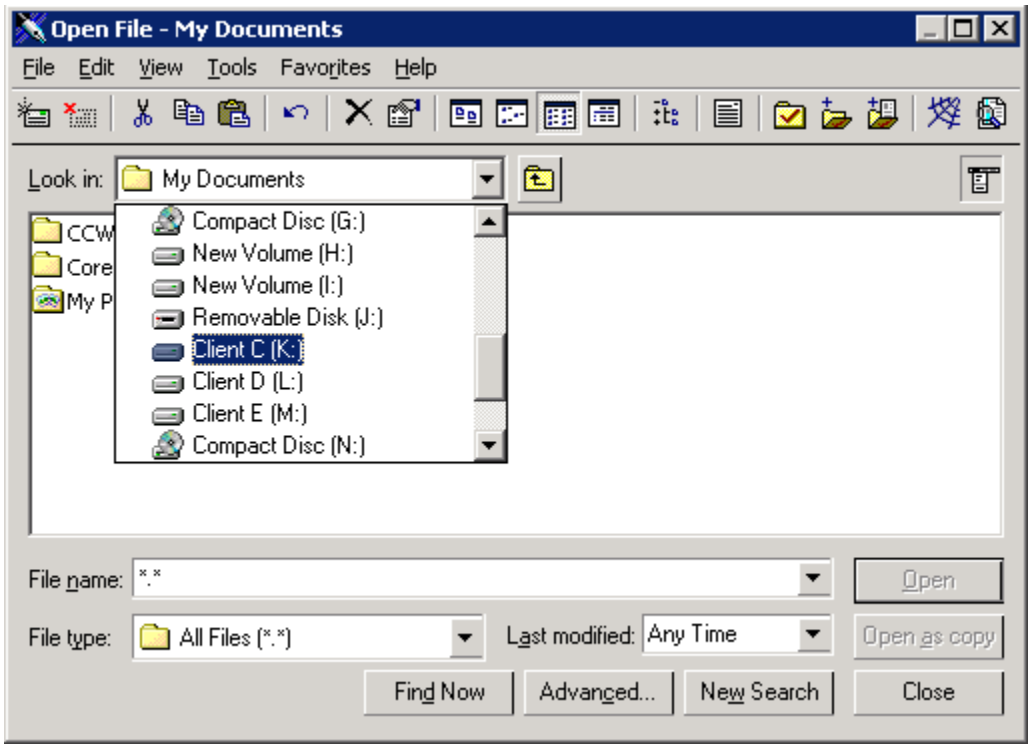
Note: Client Serial and Parallel Ports requires the loading of GO-Global libraries into session processes. This can affect the startup of a process, make some processes incompatible with GO-Global, or have fatal consequences during suspend/resume operations. For information on advanced configurations options, please consult the **Advanced Session Process Configuration** section in this guide.

To enable serial and parallel ports

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Serial and Parallel Ports** check box.
5. Click **OK**.

Client File Access

GO-Global allows users to access files stored on the client computer and to save files locally. Client drives will be listed in the application's **Open** and **Save as** dialog boxes, and are designated with a Client prefix. For example, Client C (K:), Client D (L:).



The dialog boxes list both client and host drives. Support for client drives is disabled by default.

To enable support for client drives

1. In the Cluster Manager, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Drives** check box.
5. Click **OK**.

GO-Global allows users to access USB drives. Removable drives such a floppy disks, CD ROMs, and DVD-ROMs are not supported as client drives.

Remapping Client Drives

When applications are run in GO-Global sessions with the client Drives feature enabled, GO-Global must ensure there is a one-to-one mapping between drive letters and the drives of the client and host computers. If a drive on the client and a drive on the host are assigned the same drive letter, GO-Global must assign a new drive letter to one of the drives. Client drives can be remapped by either listing them sequentially starting at a given drive letter *or* incrementing their drive letters by a specified value.

To list client drives sequentially starting at a given drive letter

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Assign consecutive letters starting at: ___**.
5. In the edit field, type the drive letter that should start the sequence.
6. Click **OK**.

For example, if a client computer has A, C, D, and H drives, and the starting point is set to drive letter M, the client's drives will be remapped respectively to M, N, O, and P. If a drive letter is already assigned to a drive, the next available letter is used. This feature is disabled by default. Once enabled, the default drive letter is M.

To increment client drive letters by a fixed value

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Increment by: ___ letters**.
5. In the edit field, type a number greater than or equal to 1 that will yield the desired offset.
6. Click **OK**.

For example, if the client computer has the same drives as above (A, C, D, and H), and the offset is 12, each of the client's drives will be incremented by 12 letters. The drives will be remapped respectively to M, O, P, and T. The default value for this setting is 12.

Hiding Client Drives

Through the Cluster Manager, administrators can hide client drives such as the client's operating system drive, floppy drive, and CD ROM drive, making them inaccessible to the user through GO-Global.

To hide one or more client drives

1. From the Cluster Manager, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. In the **Hide** box, type the client drive letters you want to hide.
5. Click **OK**.

All client drives are mapped by default. Drives listed in the **Hide** box can be listed in any order. When hiding client drives on the Linux Client and the Mac OS X Client, the user's home directory is mapped, in addition to the Root and floppy drives. For example,
Client Floppy (M:)
Client Home (N:)
Client Root (O:).

Hiding Host Drives

Microsoft's Group Policy Objects lets you hide specific host drives. For instructions, see http://support.microsoft.com/kb/231289. To hide host drives, the **Apply Group Policy** option must be enabled in the Cluster Manager's **Host Options** dialog.

Mapped Drives

Drive mappings are private within each GO-Global session. For example, if there are two sessions running on a GO-Global Host, a drive letter (H, for example) can be mapped to one network share in session 1 (e.g., \\servername\session1), and the same drive letter can be mapped to a different network share in session 2 (e.g., \\servername\session2).

Define drive letter mappings using logon scripts. You can also allow users to define their own drive letter mappings by publishing applications that provide this functionality.

Drive mappings defined within the interactive session on the GO-Global Host are not available to remote users. If all users require access to the same network share through a drive mapping, the drive mapping will generally need to be defined in a logon script.

Multi-Monitor Support

The GO-Global Client supports multiple monitors on Windows. Multi-monitor support is enabled by default, but can be disabled manually.

To disable multi-monitor support via a GO-Global shortcut

Add the argument -mm 0 from the GO-Global shortcut. For example,

gg-client.exe -h server1 -mm 0

To enable multi-monitor support via a GO-Global shortcut

Append the argument -mm 1 to the GO-Global shortcut. For example,

gg-client.exe -h server1 -mm 1

To disable multi-monitor support via a GO-Global hyperlink

Set the multimonitor parameter to false in the GO-Global hyperlink. For example,

http://hostname/goglobal/logon.html?multimonitor=false

To enable multi-monitor support via a GO-Global hyperlink

Set the multimonitor parameter to true in the GO-Global hyperlink. For example,

http://hostname/goglobal/logon.html?multimonitor=true

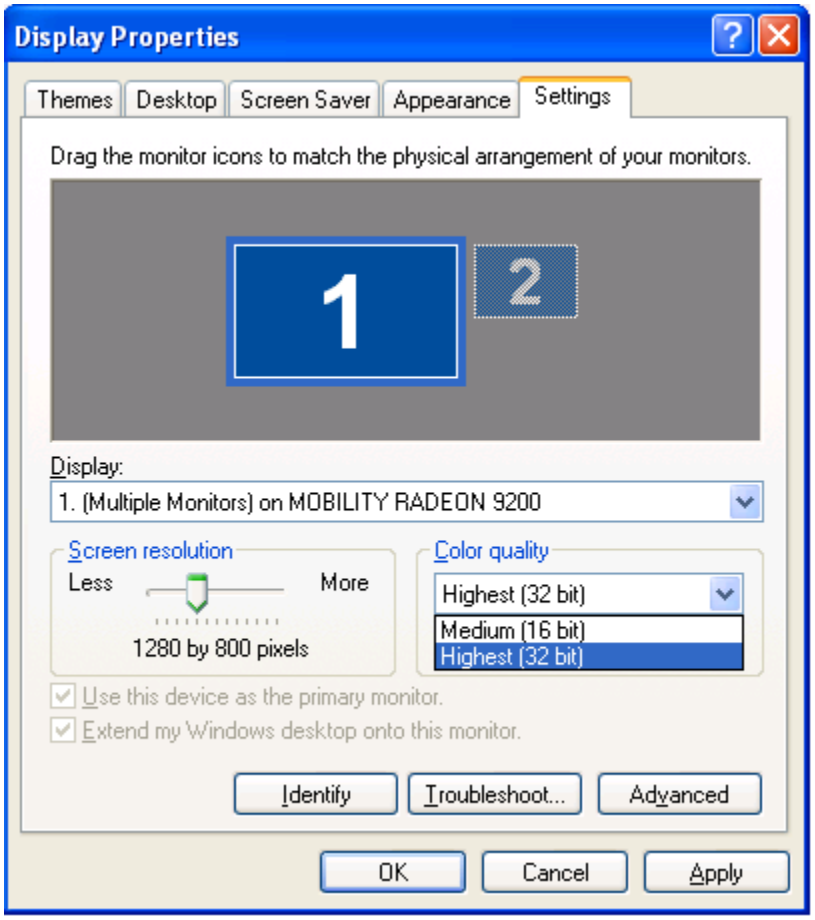
Specifying the Maximum Color Depth for GO-Global Sessions

The color depth (or color quality) of a GO-Global session can affect the quality of images in some applications. GO-Global sessions will run at the color depth of the client system up to a maximum value. By default, the maximum depth is set to 16-bits per pixel.

To increase or decrease the maximum color depth of a GO-Global session, use the –mx option when running GO-Global from a shortcut. The maximum color depth can be specified as follows: -mx 32, -mx 24, -mx 16, or -mx 8. A GO-Global session will use the minimum value of the -mx option and the color depth of the client system. For example, in order for a GO-Global session to run at 32-bits per pixel, -mx 32 must be added to the command-line and the client system must be running at 32-bits per pixel.

For example, "C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" -mx 32

When running GO-Global from a hyperlink, use the **maxbpp** parameter with the values 8, 16, 24 or 32. For example, the following hyperlink sets the maximum color depth to 24-bits per pixel: http://hostname/goglobal/logon.html?maxbpp=24



Disabling Image Compression

By default GO-Global compresses all images to a maximum of 256 colors per image. As a result, complex images may lose some sharpness. To disable image compression on GO-Global clients, append -qt 0 to the shortcut, as follows:

"C:\Program Files\GraphOn\GO-Global\Client\gg-client.exe" -qt 0

When running GO-Global from a hyperlink, set the quantize parameter to false to disable image compression. For example, http://hostname/goglobal/logon.html?quantize=false
Please note that disabling image compression will likely result in a significant increase in bandwidth sent from the GO-Global Host.

Obtaining the Name of the Client Computer

For applications that require the client's computer name rather than the GO-Global Host's, administrators can add the name of that executable under the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\GraphOn\GO-Global\Compatibility \GetComputerName** as a DWORD with a data value of **0x00000001**. Any time an executable matching any of the names listed under this registry key with a data value of **0x00000001** calls the Windows **GetComputerName** API, the given buffer will be filled in with the client's name rather than the host's.

Additionally, there is an environment variable named **CLIENTCOMPUTERNAME** that exists as part of the running environment of a published application. This environment variable contains the client's computer name. The **CLIENTCOMPUTERIPADDRESS** environment variable performs the same function, except it contains the IP Address of the client computer, rather than the computer name. The standard Windows environment variable **COMPUTERNAME** remains unchanged; its value is the host's computer name.

To obtain the name of the client computer

1. Run the Registry Editor (regedit.exe).
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **GetComputerName** key: [SOFTWARE\GraphOn\GO-Global\Compatibility\GetComputerName]
4. Create a **DWORD** entry for the executable. (For example, pw.exe).
5. Set the value of the new entry to **0x00000001**.
6. Close the Registry Editor.

When a client reconnects to a session, the CLIENTCOMPUTERNAME and CLIENTCOMPUTERIPADDRESS environment variables will be updated in each existing process once they have made an API call to acquire any environment variable. If another process attempts to acquire the environment variables of a session process prior to the session process calling one of these APIs, the value of these environment variables will not appear updated. The exact API calls that will trigger the update are:

```
UserEnv!CreateEnvironmentBlock()
Kernel32!ExpandEnvironmentStringsA/W()
Kernel32!GetEnvironmentStringsA/W()
Kernel32!GetEnvironmentVariableA/W()
```

Application Script Support

Many Win32 applications were designed for installation on a client PC and run by only one user. When an application is deployed from a GO-Global Host, multiple users need to be able to run the application simultaneously, and a number of problems may be encountered if the application is not "multi-user ready."

The best way to solve multi-user deployment problems with an application is to modify the application so it properly supports multiple users. When it is not possible to modify the application, an application script may be used to perform the pre-launch configuration and post-shutdown cleanup that is required to allow the application to run in a multi-user environment. The process for creating and deploying an application script is as follows:

1. Write a batch file that:
   - Performs the tasks necessary to prepare the application environment for a user.
   - Launches the application.
   - Performs any cleanup tasks required after the application shuts down. The batch file should end with an EXIT command. Otherwise the CMD.EXE process will not shut down.

2. Publish the application script
   a. Open the Cluster Manager.
   b. Click Tools | Applications | Add.
   c. Type the path to CMD.EXE in the **Application Path** field.
   d. In the **Command Line Options** field, specify "/K filename", where filename is the full path of the batch file to be run.
   e. Type the application display name and specify an icon.
   f. Click **OK**.

3. Test the application script
   a. Launch one of the GO-Global clients and connect to the GO-Global Host.
   b. Double-click the icon for the application script. The user interface of the application should appear on the client display, and the application should be running in the environment configured by the application script.

Note: When an application script is launched using GO-Global, the CMD.EXE window is displayed only briefly. As such, the application script cannot contain any prompts for user input.

Advanced Session Process Configuration

This section covers some of the advanced configuration options that can be set for processes running within GO-Global sessions. These settings can be applied to specific executable (.exe) applications or as default settings applied to applications without specific configurations. Care should be taken when making any changes discussed in this section. An incorrect configuration can affect the startup of a process, make a process incompatible with GO-Global, or have fatal consequences during suspend/resume operations.

Most applications that run within a GO-Global session will have GO-Global libraries loaded within them to perform redirection in order to obtain desired behavior. There are two levels of redirection that these libraries can initialize.

The first level configures application and system modules to behave in a particular way. Most applications will need one or more level one settings enabled. Level one settings include Client Time Zone, Client Printing, and altered Windows API behavior.

The second level creates a communications channel between the application and client for duplex transmission of session related information. For the highest level of application compatibility with GO-Global, level two settings should be enabled in as few applications as possible. Level two settings include Client Sound and Client Serial and Parallel Ports.

The different configuration settings employed by the GO-Global libraries that redirect session processes are controlled by hexadecimal bit values within the registry. A bitwise OR operation is performed on the desired bit values to create a DWORD registry value.

Here is the documented list of process redirector bits and a description of what they configure.

0x00000001* - Prohibit a process from running within a session

0x00000002 - Disable the loading of GO-Global libraries. All redirection will be disabled. The time required to perform the redirection operations is generally a small percentage of the time required to launch typical Windows applications, but it can be a large percentage of the time required to launch and run simple console applications. Some console applications do not require redirection and performing these tasks can significantly extend the time required to execute logon scripts. Including this bit allows administrators to bypass redirection of a process. Applications execute faster since the GO-Global libraries are not loaded and initialized. This bit can also be used for applications that, for one reason or another, are incompatible with some or all of the GO-Global redirection settings.

0x00000004 - Disable Client Time Zone. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Time Zone redirection settings.

0x00000008 - Disable Client Printing. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Printing redirection settings.

0x00000010* - Disable the use of the GO-Global 'UI' skin module.

0x00000020* - Enable the use of the GO-Global 'UI' skin module.

0x00000080* - Enable the Windows ProcessIdToSessionId() API to return the GO-Global session ID.

0x00000100* - On 64-bit systems, enable the Windows ProcessIdToSessionId() API to return the GO-Global session ID for 32-bit processes only. This is required for printing to work in 32-bit processes on 64-bit systems. Including this bit in settings for 64-bit processes has no effect.

0x00000200 - Disable Client Sound. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Sound redirection settings.

0x00000400 - Disable client Serial and Parallel Ports. This bit can be used for applications that, for one reason or another, are incompatible with the GO-Global Client Serial and Parallel Ports redirection settings.

0x00000800* - Enable the Windows GetComputerName() API to return the client computer name. See also: Obtaining the Name of the Client Computer. Disable the updating of the client environment variables (CLIENTCOMPUTERNAME and CLIENTCOMPUTERIPADDRESS) when a client reconnects to a suspended session.

0x00001000* - Disable, for optimization purposes, some of the normal processing performed when Explorer.exe is launched. This bit prevents Explorer.exe from launching processes listed under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, RunOnce and RunOnceEx registry keys. This reduces the system resources needed to run Explorer in a session.

0x80000000* - Enable application produced with Delphi to use the Client Serial and Parallel Ports feature. Applications built with Delphi do not properly process all return values from the Windows GetOverlappedResult() API. This bit prevents the returning of WAIT_TIMEOUT and instead returns WAIT_OBJECT_0.

* Indicates advanced options that should only be used if instructed to by your support contact.

Note:	All the unlisted bits are purposely undocumented and reserved for internal GraphOn use only. Do not alter any registry values that contain any unlisted bits and do not apply any unlisted bits to any registry values you add. GO-Global Host operation will be compromised if this is done.

These bits can be combined to customize the redirector settings of specific applications or to change the default settings used by applications that do not have a registry entry. In either case always include the default value bits set by the initial install of GO-Global, unless instructed otherwise by a support engineer.

To add custom redirector settings for a specific application

1. Click Start | Run.
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\GraphOn\GO-Global\Loader\Processes.
4. Click Edit | New | DWORD value.
5. Type the name of the application's executable file. (For example, Beeps.exe.) The application's name can be specified as either a fully qualified path or as the file's base name and extension.
6. Select the new registry value.
7. Click Edit | Modify.
8. Verify that the Base selection is Hexadecimal.
9. Type the combined bits in the **Value data** edit box.
10. Click **OK**.

To change the default redirection settings

1. Click Start | Run
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\GraphOn\GO-Global\Loader\Processes.
4. Select the existing **DefaultLoaderOptions** registry value.
5. Click Edit | Modify.
6. Verify that the Base selection is Hexadecimal.
7. Type the new setting in the **Value data** edit box.
8. Click **OK**.

Example Configuration

A GO-Global host has the following applications installed and registered in the Cluster Manager.

- DataDownloader.exe
- DataProcessor.exe
- DataViewer.exe

The DataDownloader.exe executable is a Windows application that reads data from a serial device and saves it to a file. Client Sound is needed for error conditions alerts that can be signaled while data is being downloaded. Client Files Access will be used to store the data file on the client system. The Windows GetComputerName() API must be redirected so that the client computer name can be used to indicate the source of the data within the data file.

Because the serial device that contains the data is connected to the client computer, Client Serial and Parallel Ports will need to be enabled. Because this is the only process that will access Client Serial and Parallel Ports on this system, a registry entry specifically for DataDownloader.exe has been added. This minimizes the risks and overhead associated with this level two redirector setting by disabling Client Serial and Parallel Ports in all other applications.

The settings for this application are calculated as follows:

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000800 - This is the bit that enables the Windows GetComputerName() API redirection.

0x00000910 – This is the hexadecimal DWORD to be set in the DataDownloader.exe registry value.

The DataProcessor.exe executable is a console application that needs Client File Access to read in the serial data file from the client and write out the processed data file to the client. It will also use Client Time Zone to properly process the times recorded in the serial data file. All other settings will be disabled to minimize the risks and overhead associated with redirector settings.

The settings for this application are calculated as follows:

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000008 - This is the bit that disables Client Printing.

0x00000200 - This is the bit that disables Client Sound.

0x00000400 - This is the bit that disables Client Serial and Parallel Ports.

0x00000718 – This is the hexadecimal DWORD to be set in the DataProcessor.exe registry value.

The DataViewer.exe executable is a Windows application that displays the data so that it can be analyzed. It needs Client File Access to read in the processed data file from the client. It needs Client Sound so that application sounds can be heard. It needs Client Printing so that the analyzed data can be printed on paper. These are some of the settings needed by most applications, so the DefaultLoaderOptions registry value is used for the calculation below.

The default setting will be changed to disable the Client Serial and Parallel Ports. This can be done because the only application that uses Client Serial and Parallel Ports, DataDownloader.exe, has its own registry setting that specifically enables it.

0x00000110 - These are the bits originally set in DefaultLoaderOptions.

0x00000400 - This is the bit that disables Client Serial and Parallel Ports.

0x00000510 – This is the hexadecimal DWORD to be set in the DefaultLoaderOptions registry value.

This example demonstrates how a combination of application specific and the default settings can be used to minimize the risk of application incompatibilities and allow an optimal environment to run in.

Proxy Tunneling

Proxy tunneling via the **HTTP CONNECT** method allows a user who accesses the Internet via a proxy server to connect to GO-Global Hosts on the Internet when the following conditions are met:

- The user runs the GO-Global Client on a Windows computer;
- The address and port of the proxy server are stored under the client computer's Internet Options; and
- The proxy server is configured to allow HTTP CONNECT method tunnels to the port on which the GO-Global Host is configured to accept RapidX Protocol (RXP) connections.

Proxy Tunneling via the HTTP CONNECT Method

When users on Windows computers are unable to establish a direct connection to a GO-Global Host, and when the client computer is configured through its Internet Options to use a proxy server, GO-Global attempts to establish an HTTP CONNECT method tunnel to the GO-Global Host.

Specifically, the client:

1. Connects to the proxy server using the address and port specified in the client computer's **Internet Options**.
2. Sends a CONNECT request to the proxy server: i.e., CONNECT *address:port* HTTP/1.0, where *address* and *port* are respectively the IP address of the GO-Global Host and the port on which the server accepts RXP connections (e.g., 491 by default).
3. Reads the reply from the proxy server.
4. Responds to the proxy server's reply as follows:
    a. If Basic authentication is required, GO-Global prompts users for their user name and password and then repeats Step 2, this time providing the user's credentials.
    b. If the request failed, GO-Global displays the following message: "Failed to connect to serverAddress via the proxy server at proxyAddress : [reason for failure].
    c. If the request succeeded, GO-Global initializes the RXP connection and starts the session.

To allow HTTP CONNECT method tunnels using port 443

1. Configure the GO-Global Host to accept connections on port 443.
2. Specify port 443 in the GO-Global hyperlink.
3. If necessary, configure the proxy server to allow connections to the GO-Global Host on ports 80 (HTTP) and 443 (HTTPS).

Once you have configured the GO-Global Host and the GO-Global hyperlinks, users that meet the three requirements above will be able to connect to the host. Users running GO-Global from a shortcut will need to append the -hp argument followed by 443 to the shortcut. For example, "...\gg-client.exe" -h server -hp 443. Otherwise these users will be unable to sign in to GO-Global.

Notes:

GO-Global clients are unable to connect to GO-Global Hosts via proxy servers that are configured to verify that the traffic on port 443 is HTTPS.

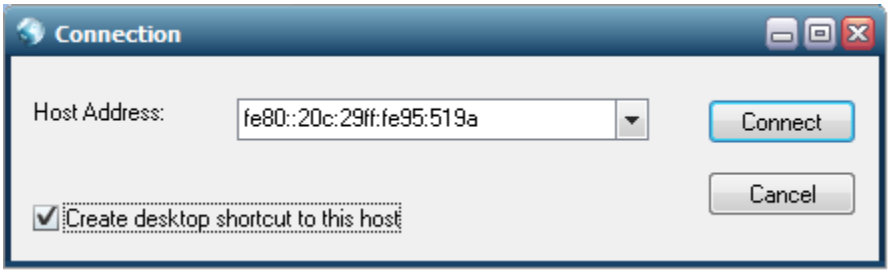
In a proxy server configuration, GO-Global only supports Basic authentication.

Support for Internet Protocol version 6

GO-Global supports Internet Protocol version 6 (IPv6), the successor to IPv4, the dominant Internet layer protocol. IPv6 has a much larger address space than IPv4, and allows flexibility in allocating addresses and routing traffic.

GO-Global supports the following:

- GO-Global Hosts accepts connections from IPv4 and IPv6 clients.
- GO-Global relay servers accept connections from IPv4 and IPv6 dependent hosts.
- Administrators can specify a relay server in the Cluster Manager using a hostname, an IPv4 address, or an IPv6 address.
- Users can connect to a GO-Global Host using its hostname, its IPv4 address, or its IPv6 address.



Enabling Support for PAE

On Windows Server 2008, Windows Server 2003, and Windows XP Professional, GO-Global supports memory in excess of 4 GB by way of the Physical Addressing Extension (PAE).

To enable PAE

1. Click Start | Run.
2. Type **C:\boot.ini**, where X is the drive letter of the location of the boot files, tldr, Boot.ini, and so forth.
3. Modify the line that corresponds to your operating system by appending the switch /PAE.
4. Save the file, and restart the computer.

Performance Auto-Tuning

Performance auto-tuning is used in situations when an application is generating a large amount of graphical data or when a client system has limited processing speed. When Performance auto-tuning is enabled, the client machine reports the rate at which it is processing the data the host is sending. The host uses this information to reduce the total amount of data it sends by eliminating any graphical information that the client system is unable to keep up with, such as animations with a high frame rate, or by choosing to send an image of an application's contents rather than primitive graphical operations.

Performance auto-tuning allows any client to run even the most graphically intense applications. Performance auto-tuning is disabled by default.

To enable Performance Auto-Tuning for all clients connecting to a host

1. Locate the file **HostProperties.xml** in one of the following directories: C:\Documents and Settings\All Users\Application Data\GraphOn (On Windows XP and Windows 2003); C:\ProgramData\GraphOn (On Windows Vista, Windows 2008 and later).
2. Open **HostProperties.xml** in Wordpad and locate the following section:

```
</property>
- <property id="ClientProcessingBatch" group="Miscellaneous"
type="UINT32">
<value>0</value>
</property>
```

3. Change the **ClientProcessingBatch** value from 0 to 1.
4. Stop and start the **GO-Global Application Publishing** Service.

Note: Make sure to create a backup of **HostProperties.xml** before making any changes.

Automatic Windows Update and Hotfix Compatibility

GO-Global supports High Priority Windows Updates, Windows Hotfixes, and Windows Service Packs. GraphOn tests GO-Global for compatibility with High Priority Windows Updates and Windows Service Packs. Certification testing begins as soon as the High Priority Windows Update or Service Pack is released and is usually completed within one day.

If GraphOn certifies that the Windows Update or Service Pack is compatible with the currently released version of GO-Global, Updates or Service Packs can safely be installed on GO-Global Hosts.

Microsoft does not release Windows Hotfixes from its Microsoft Update site and typically only provides Hotfixes to customers on an as-needed basis. Since Hotfixes are not universally available, GraphOn does not run compatibility tests on Windows Hotfixes.

GO-Global is expected to be compatible with nearly all future Windows Updates and Hotfixes. Windows Service Packs, however, contain more significant changes and may not be compatible with GO-Global. If a Windows Update, Hotfix, or Service Pack is incompatible with GO-Global, the Application Publishing Service will record an error in its log file and close. If this occurs, contact Customer Support. GraphOn will typically provide support for incompatible updates within one week.

GraphOn recommends that users install only Windows Updates and Service Packs on GO-Global Hosts that have been certified to be compatible with GO-Global. As such, GraphOn recommends that GO-Global Hosts be configured so they do not automatically install Windows Updates.

To disable the automatic installation of Windows Updates

1. Click Start | Control Panel.
2. Click Automatic Updates.
3. In the **Automatic Updates** dialog, click one of the following options:
   - **Download updates for me, but let me choose when to install them.**
   - **Notify me but don't automatically download or install them.**
   - **Turn off Automatic Updates.**
4. Click **OK**.

Silent Installation

The GO-Global client can be installed silently. In other words, installation is performed without user interaction except for the initial launch of the process.

To run a silent install

1. Run cmd.exe as local administrator (Run as administrator).
2. Run the following command:
   cmd /c gg-client.windows.exe /s /v"/qn"

This adds the GO-Global shortcut to the Start menu under Start | Programs | GraphOn GO-Global 4 | GO-Global.

To install the GO-Global web clients, but not the shortcut to the native client, run the following command:

cmd /c gg-client.windows.x86.exe /s /v"/qn GOGLOBAL_SHORTCUT="No""

Log Files

The GO-Global Host creates log files in which it records information about its own performance and that of certain GO-Global processes. GraphOn Technical Support uses the data to diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or host machine, are located in the **Log** folder on the GO-Global Host. For example, D:\Program Files\GraphOn\GO-Global\Log. In the Log folder are three subfolders: **Backup**, **Codes**, and **Templates**. Be careful not to delete these folders. GO-Global messages are recorded within log files prefixed with *aps* and followed by the date and time (to the nearest millisecond) the Application Publishing Service was started. (For example, aps_2011-04-04_09-55-47-636.html). A new log file is created each time the Application Publishing Service is started. The log file with the latest date and time stamp contains messages for the current, or most recent instance of the Application Publishing Service.

Problems detected in the execution of GO-Global are described by entries in the log file. Each entry is uniquely identified by an item number along with a date and time stamp, and a description of the event or program error. GraphOn Technical Support uses this information to locate a problem's source and to determine its resolution.

Entries in the log file may also include prefixes for locating messages associated with an individual user's session and applications. If the event occurred within the context of a given session, the name of the session will appear at the beginning of the message, for example, *SuzyG on Server1*. If the event occurred within the context of a connection to the Application Publishing Service—a connection either from a client or from an application, the name of the connected process will be included in the message prefix, for example, *pw (1244).* In this example, a problem occurred during the connection between the Program Window process and the Application Publishing Service. 1244 is the ID of the process in which the event took place. If the message prefix contains the connection name *aps*, the event occurred within the Application Publishing Service, but was not associated with a connection to another process.

Selecting a New Location for the Log Files

By default, log files are created and stored at \Program Files\GraphOn\GO-Global\Log. You can select a new location for the log files through the Cluster Manager's **Host Options** dialog.

To select a new location for the Log files

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Log**.
3. Type the path to the new directory in the **Folder** edit box or browse to its location.

You cannot specify a path to a remote system for the log file location. For example, if you type a UNC path or a mapped network drive in the **Folder** edit box, the following message is displayed:

"Please specify a usable Windows folder where log files may be written."

Note: You should move the **Backup** folder and existing log files to the new location, along with the **Templates** and **Codes** subfolders.

Setting the Output Level

GO-Global offers six log output levels, as follows:
0: No output
1: Errors
2: Errors and Events
3: Errors, Events, and Warnings
4: Errors, Events, Warnings, and Diagnostic Messages
5, 6: Errors, Events, Warnings, Diagnostic Messages, and Trace Messages

To set the output level

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Log**.
3. Type one of the above numeric values in the **Output level** box.
4. Click **OK**.

CAUTION! Setting the log output value to 5 or 6 will cause the host to generate very large log files and may adversely affect performance and scalability. These output levels should only be used in a controlled environment—preferably when no clients are accessing the GO-Global Host.

The default value for the Output level is 4.

Maintaining Log Files

GO-Global creates a new log file in the **Log** folder every time the Application Publishing Service starts. Over time these files can accumulate and consume a significant amount of disk space. To help manage these files, GO-Global lets you delete or backup log files and set file size or age limits.

To delete log files

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select **Delete**.
4. Specify how old (in days) log files can become before being deleted.
5. Specify at what size (in megabytes) log files are to be deleted.
6. Click **OK**.
7. Restart the **GO-Global Application Publishing Service**.

To backup log files

1. From the Cluster Manager, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select **Back up**.
4. Specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
5. Specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
6. Click **OK**.
7. Restart the **GO-Global Application Publishing Service**.

Once every half hour, and each time it is started, the Application Publishing Service searches the **Log** folder for files that have reached the specified age or size limit. It then either deletes the files or moves them to the **Backup** subdirectory of the Log folder. If while sweeping the log files, the Application Publishing Service finds that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

By default, log files are backed up after 7 days or when the file size has reached 20 MB.

Support Request Wizard

The GO-Global Host includes a Support Request Wizard that gathers log files and information about the host that can be sent to technical support. Administrators can run the Support Request Wizard from the Cluster Manager by clicking Help | Support Request Wizard or via the Start menu by clicking Programs | GraphOn Global 4 | Tools | Support Request Wizard.

The wizard prompts the administrator for a description of the problem, a time frame for when the problem happened, and the user or users that were affected. If the issue is associated with an existing support case, administrators can enter the Case Number. By default, the zipped report is placed on the user profile's desktop, but administrators can select an alternative destination via the wizard.

Administrators can upload the zipped file to the support ticket via the GO-Global support portal http://www.graphon.com/customer-support/graphon-customer-support-portal or reply to an existing support email (support@graphon.com) with the attachment.

INDEX

A

-a, 46, 66
-ac, 46, 79, 81
Active Directory, 39, 72, 78
Active Directory Domain, 76
Active Directory Domain Controller, 39
Active Sessions, 76
All Hosts, 24, 49, 73, 80, 86
allclients.html, 7
Always in front, 50
Application Publishing Service, 6, 21, 24, 38, 71, 72, 74, 100, 102
Application Script Support, 93
Application Users/Groups, 26
Applications, 47
  adding, 25
  duplicating, 27
  editing properties, 27
  installing, 25
  removing, 28
  renaming, 27
aps, 100
ARGS, 59
Audio support, 87
Authentication, 39
autoclosebrowser, 59
autoconfigprinters, 59
Automatic client updates, 63

B

Backup, 102
Backup folder, 101
Basic authentication, 97
BLM, 13
Broadcast Interval, 49
Browser Logons, iii, 7

C

-c, 66
CA, 36
CA certificate, 32, 34
CA key, 32, 33
ca.cfg, 34
ca.crt, 34, 35
Cache password on the client, 41
Cache passwords, 41
Cache passwords on the host, 44
Cached password, 42
Case Number, 102
CD ROMs, 88
Central license server, 6, 12
Certificate Authority, 30
Certificate Signing Request, 31, 33, 35, 36
Certificate Wizard, 36
Change Icon, 25, 27
Change Password, 43, 44
Client clipboard, 86
Client Connections, 76
Client drive letters, 89
Client drives, 88, 89
Client file access, 1, 65, 88, 96
Client keyboards, 13
Client printer name, 86
Client Printer Naming, 86
Client printers, 59
Client printing, 79, 93
Client Serial and Parallel Ports, 87
Client Sound, 3, 87, 96
Client Time Zone, 93
Client updates, 63
CLIENTCOMPUTERIPADDRESS, 92
CLIENTCOMPUTERNAME, 92
clients.html, 7
Client-side password caching, iv, 41
Clipboard support, 86
Cluster Manager, 24, 25, 26, 27, 44, 71, 73
  accessing, 24
  accessing from a client machine, 55

refreshing, 48
cm.exe, 55
Codes, 101
Color depth, 4, 91
Command-line arguments, 46, 66
Command-line options, 25, 27, 28
Common Name, 31, 34, 35
Compression, 59, 66
Connected Clients, 30, 47
Connection dialog, 38, 66, 71
Consecutive letters, 89
Copy and paste, 86
CPU, 49
CPU requirements, 4
CPU utilization, 48
Cross-platform compatibility, 1

D

DataDownloader.exe, 95
DataProcessor.exe, 95
DataViewer.exe, 95
Default printer, 81, 82, 85
DefaultLoaderOptions, 96
Delegation, 39, 77
Delegation Support, 76
Demilitarized zone, 72
Demo license, 5
Dependent application server, 75
Dependent host, 70, 73
Dependent hosts, 74
DES encryption, 37
Diagnostic Messages, 101
Disconnect, 44, 45, 53
Disconnecting a session, 45
Display name, 25, 66
DMZ, 75
DNS servers, 76
Domain Controller Security Policy, 21
Domain name, 21
Domain Name System, 76
Domain Security Policy, 21
DPAPI, 41
Drive Letter Mapping, 2
Drive letters, 89
Drive mappings, 90
DVD-ROMs, 88
DWORD, 94

E

Encryption, 37
Errors, 101
Events, 101
Executable Path, 25, 26, 27
Explorer.exe, 94

F

Failover server, 74
Failure recovery, 74
Fallback Layout Text, 19
FAT file system, 25, 28
File Permissions, 22
Firewall, 3, 13, 38, 72, 75
FLEXnet, 13
floppy disks, 88

G

geometry, 61
GetComputerName, 92
gg-client.windows.exe, 63
GGII, 18
ggw.exe, 66, 68
Global logon script, 51
Global scripts, 50
Go Daddy, 32
GO-Global Application Publishing Service, 6, 39, 77, 78
GO-Global Client, 66
GO-Global Client.msi, 100
GO-Global Host, iii, 3, 7, 21, 22, 29, 44, 93, 101
GO-Global Host Performance Counters, 76
GO-Global Input Identifiers, 18
GO-Global libraries, 87
GO-Global License Manager, 12
GO-Global shortcut, 60
Grace period, 55
Group Policy, 49
Group Policy Support, 2

H

-h, 66
Hiding client drives, 89
Host, 5
Host activity, 47
Host monitoring, 1
Host Options dialog, 45
Host Port, 38
hostid, 10
HTTP, 97
HTTP CONNECT method, 96
HTTPS, 97
Hyperlinks, 9

I

Idle limit, 53
Idle time, 53
IIS, 7, 9
Image compression, 92
IME, 13
Inactivity Timeout, 2
inbrowserprocess, 60
Increment, 89
Independent hosts, 70, 71
index.htm, 7
Input Method Editors, 13
installCE.html, 7
Installing the GO-Global Host, 5
installLinux.html, 7
installMac.html, 7
installWindows.html, 7
Integrated Windows authentication, 39, 45, 72, 73, 76
Integrated Windows Authentication, 44

INTERACTIVE group, 39
Intermediary certificate, 32
Internet Options, 32, 96
IP address, 47
IPv4, 98
IPv6, 38, 98
isembeddedwin, 59

K

Kerberos authentication protocol, 76
Keyboard layout, 18
Keyboard Mapping Files, 16

L

Launch Parameters, 27
Layout text, 18
Layout text substitutions, 18
License Manager Port, 13
License Retrieval Wizard, 5, 6
License server, 12
License-file list, 10
License-file list redundancy, 11
Linux Client, 58
Live collaboration, 29
LM_LICENSE_FILE, 10, 11, 12, 13
lmtools, 11
Load balancing, 2, 70
Local logon rights, 21
Local Security Policy, 21
Locality, 31
Locality Name, 34, 35
Log Files, 100, 102
Log folder, 102
Log Folder, 72
Logon dialog, 60, 66
Logon Manager, 50
Logon scripts, 50, 90

M

Maintenance, 102
Mapped drive, 26
Mapped drives, 90
MappedPrinterDrivers.xml, 81, 84, 85
Master, 10
Maximum number of sessions, 52, 75
Maximum sessions, 74
Maximum Sessions, 76
Maximum sessions count, 52
MEM, 49
Mem usage, 48
Memory, 98
Memory requirements, 4
Messages, 100
Microsoft Cluster Service, 74
Microsoft Internet Information Server, 9
Microsoft Management Console, 36
MIME Type, 9
Modifying the Host Port Setting, 38
Multiple Input Locales, 19
Multi-user deployment, 25, 93

N

NETWORK group, 39
Network Printer, 23
network share, 90
New Password, 42, 43
noscale, 60
NTFS, 22, 25, 28

O

ODBC data sources, 26
OpenSSL toolkit, 31, 32
Options dialog, 56
Organization Name, 34, 35
Organizational Unit, 31
Organizational Unit Name, 34, 35
Output Level, 101

P

-p, 66
PAE, 98
Pan buttons, 69
Password Caching, iv, 40
Password Change, 42, 44
Password Locations, 42
Passwords, 67
PEM format, 36
Performance Auto-Tuning, vii, 98
Performance counters, 2, 75
Performance problems, 52
Physical Addressing Extension, 98
Physical memory, 53
PlaySound, 3, 87
Pocket PC Client, 68
Port, 38
Port 491, 3, 70
Port 80, 70
Preview PDF, 80
Print Spooler Service, 79
Printer Configuration, 81
Printer drivers, 79, 84, 85
Printer settings, 82
printerconfig, 79, 81
PrinterNameFormat, 86
Printers Applet, 81, 82, 83
Process
  ending, 29
Process ID, 47, 100
Process information, 47
Processes, 49
Procs, 48
Product Code, 5
Program Window, 26, 27, 44, 81
Progress message, 49
Progress Messages, 49
proxy printer, 85
Proxy printer names, 86
proxy printers, 81
Proxy server, 97
Proxy tunneling, 2, 96

R

-r, 46, 66
RapidX Protocol, 96
Red x, 24, 72
Redirection settings, 95
Redundant license lervers, 10
Refresh rate, 48
Relay server, 71, 72, 73, 74, 75
Remapping client drives, 89
Remote Registry Service, 75
Removable drives, 88
Reset Printers, 83
Resource limits, 49, 52
Roaming user profiles, 22, 70
RSA algorithm, 41
RSA private key, 33

S

Secure Socket Layer, 30
Security, 21, 37
Security Alert, 36
Security Rollup Package, 3
Serial and Parallel Ports, 87, 93, 96
Server Connections, 76
Server keys, 35
Server Performance Counters, 76
server.cfg, 34
server.crt, 33, 35
server.key, 33, 35
Server-side password caching, iv, 40, 76
Service Principle Name, 78
Session
  encrypting, 37
  terminating, 29
Session information, 47
Session limit, 53
Session Name, 47
Session Process Configuration, 93
Session reconnect, 2, 44, 71
Session shadowing, 2, 29
Session Startup, 51
Session termination, 45
Session timeout, 44
Sessions, 48, 49
Sessions tab, 45
Shadowing a session, 29
Shared account, 46, 47
Silent installation, 100
sndPlaySound, 3, 87
Sound, 87
Sound card, 87
Spaces, 67
SSL, 30
SSL Certificate, 30, 31, 33, 36, 37
SSL Security, 2
SSL transport, 36
Standard authentication, 39, 40
Start Directory, 25, 26, 27, 28
Start menu, 57, 58, 65
Startup parameters, 66
Startup State, 25, 27, 28
Startup Time, 47
Status bar, 48, 49, 56
Support Request Wizard, 102
Support ticket, 102
System requirements, 3

T

TCP, 30
TCP packets, 3
TCP/IP, 3, 70
Templates, 101
Terminal Connection Manager, 67
Test Page, 83
Three-server redundancy, 10
Trace Messages, 101
Transmission Control Protocol, 30

U

-u, 66
UNC, 26
Universal Driver, 79
Universal Printer Driver, 80, 83, 84
USB drives, 88
User, 47
User Accounts, 21
User Profiles, 22
User roaming, 2
User-specific scripts, 50

V

Virtual memory, 53

W

Warning period, 54
Warnings, 101
waveOut, 3, 87
Web access, vi, 61
Web folder, 7
Web proxy server, 96
Windows 7, 3
Windows CE Client, 66
Windows Client, 57, 66
Windows Explorer, 22
Windows folder, 79
Windows Mobile, 68
Windows Performance Monitor, 75
Windows Printer Drivers, 80
Windows Server 2003, 9
Windows shortcut, 66
Windows Vista, 3
WoW64, 3

Y

Yellow x, 72

Z

Zoom buttons, 69